(19)日本国特許庁（ＪＰ）　(12)**公表特許公報（Ａ）**　(11)特許出願公表番号
特表2003－500722
（P2003－500722A）
(43)公表日　平成15年１月７日(2003.1.7)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　1/00		Ｇ０６Ｆ　15/00	３３０Ｆ	５Ｂ０７６
15/00	３３０	9/06	６６０Ｄ	５Ｂ０８５

審査請求　未請求　予備審査請求　有　（全166頁）

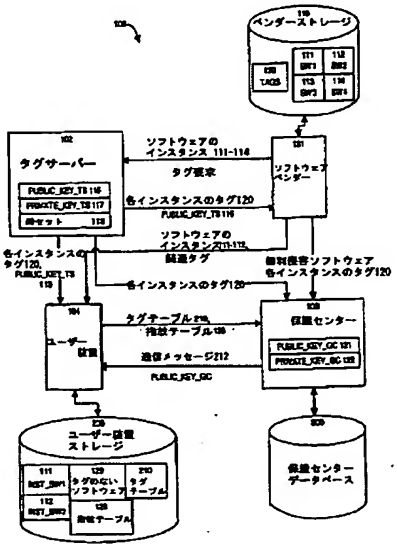
(21)出願番号　特願2000－620446(P2000－620446)
(86)（22)出願日　平成12年５月２日(2000.5.2)
(85)翻訳文提出日　平成13年11月５日(2001.11.5)
(86)国際出願番号　ＰＣＴ／ＵＳ００／１１８２１
(87)国際公開番号　ＷＯ００／０７２１１９
(87)国際公開日　平成12年11月30日(2000.11.30)
(31)優先権主張番号　０９／３０５，５７２
(32)優先日　平成11年５月５日(1999.5.5)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ラビン・マイケル・オー
ＲＡＢＩＮ，Ｍｉｃｈａｅｌ，Ｏ.
アメリカ合衆国，マサチューセッツ州　02138，ケンブリッジ，コンコード　アベニュー　243
(71)出願人　シャーシャ・デニス・イー
ＳＨＡＳＨＡ，Ｄｅｎｎｉｓ，Ｅ.
アメリカ合衆国，ニューヨーク州　10012，ニューヨーク，ブリーカー　ストリート　100
(74)代理人　弁理士　杉本　修司　（外２名）

最終頁に続く

(54)【発明の名称】　情報保護方法および装置

(57)【要約】
ソフトウエアのオーナーおよびベンダーが知的所有権を保護し、使用料を請求できるための方法と装置。このシステムはソフトウエアのすべてのインスタンス（事例）ごとに特有のタグを作成する。各ユーザ装置は管理プログラムを実行し、タグを使用して、ソフトウエアオーナーの権利を侵害するソフトウエアのインスタンスが使用されないことを保証する。ソフトウエアのインスタンスをインストールまたは使用するとき、管理プログラムは関連タグを確認し、そのタグを格納する。タグ付けされていないソフトウエアをインストールまたは使用すると、管理プログラムはソフトウエアの選択された部分の指紋付けし、その指紋を格納する。ユーザ装置の管理プログラムは定期的に呼び出しするか、または保護センターにより呼び出しされる。保護センターは、現在の呼び出しデータと過去の呼び出し記録とを比較してソフトウエアの無許可使用を検出する。保護センターは管理したソフトウエアのインスタンスの継続使用を有効または無効にして、その呼び出しを完了する。



【特許請求の範囲】

【請求項１】　ソフトウエアの使用を管理するためのシステムであって、

ソフトウエアのインスタンスを作成するソフトウエアベンダーと、

複数のタグを作成するタグサーバーであって、そのタグはソフトウエアのインスタンスごとに１つ存在し、各タグは、そのタグが関連しているソフトウエアのインスタンスを一意に識別するタグサーバーと、

ソフトウエアのインスタンスを受け取ってインストールし、さらにそのソフトウエアのインスタンスに一意に関連するタグを安全に受け取るユーザー装置であって、ソフトウエアのインスタンスの使用を検出し、ソフトウエアのインスタンスに関連するタグの認証を確認した後、そのソフトウエアのインスタンスの使用を許可する管理プログラムを含むユーザー装置とを備えているシステム。

【請求項２】　請求項１において、ユーザー装置上の前記管理プログラムがタグの認証を確認し、タグテーブル内にそのタグを維持し、そのタグが認証されている場合は前記ソフトウエアのインスタンスを維持し、ソフトウエアに関連するタグが認証されていない場合はソフトウエアのインスタンスを拒絶するシステム。

【請求項３】　請求項２において、前記管理プログラムがタグ内のハッシュ関数値を確認して、そのタグが認証されているかどうか、さらに前記ソフトウエアのインスタンスに適正に関連付けされているかどうかを決定するシステム。

【請求項４】　請求項２において、前記タグがデジタル的に署名され、前記管理プログラムがタグのデジタル署名を確認することによりタグの認証を確認するシステム。

【請求項５】　請求項１において、タグサーバーにより作成された複数のタグのそれぞれが、少なくとも１つのソフトウエア名と、ソフトウエアのインスタンスの固有の番号と、ソフトウエアのインスタンスの各部分のハッシュ関数値を含んでいるシステム。

【請求項６】　請求項５において、前記ソフトウエアのインスタンスの固有の番号が疎セットから選択されているシステム。

【請求項７】　請求項５において、各タグが前記管理プログラムの固有の識

別子をさらに含んでいるシステム。

【請求項８】　請求項７において、前記管理プログラムが、タグ内の管理プログラムの前記固有の識別子がユーザー装置上の管理プログラムの識別子と同一であることを確認するシステム。

【請求項９】　請求項１において、各タグが、そのタグに関連した前記ソフトウエアのインスタンスの各部分で計算された少なくとも１つの指紋を含んでいるシステム。

【請求項１０】　請求項９において、前記管理プログラムにより、タグに関連したソフトウエアのインスタンスが、そのソフトウエアのインスタンスに関連したタグ内に含まれる少なくとも１つの指紋に対する同一位置指紋検査を満たすことを確認するシステム。

【請求項１１】　請求項１０において、前記同一位置指紋検査が、ソフトウエアのインスタンスの使用の前、使用中、および使用後において少なくとも１回前記管理プログラムにより実行されるシステム。

【請求項１２】　請求項９において、各タグが、少なくとも１つの指紋を計算できる値を含む少なくとも１つの位置のリストをさらに含み、前記管理プログラムにより、各タグに関連したソフトウエアのインスタンスが、前記少なくとも１つの位置のリスト内で指定された位置におけるソフトウエアに関連する少なくとも１つの指紋に対する同一位置指紋検査を満たすことを確認するシステム。

【請求項１３】　請求項１において、前記ソフトウエアのインスタンスによりすべてのデータファイルがアクセスされ、そのアクセスを実行するソフトウエアのインスタンスに関連する情報が前記データファイルに関連する位置に格納されているシステム。

【請求項１４】　請求項１３において、ソフトウエアのインスタンスに関連する前記情報が、そのソフトウエアのインスタンスに関連するタグであるシステム。

【請求項１５】　請求項１３において、ソフトウエアのインスタンスに関連する前記情報が、そのソフトウエアのインスタンスにより実行される変更の時刻であるシステム。

【請求項１６】　請求項１３において、前記アクセスを実行するソフトウエアのインスタンスに関連する前記情報が、前記管理プログラムだけがアクセス可能な安全な位置に書き込まれているシステム。

【請求項１７】　請求項１６において、前記管理プログラムが、ソフトウエアのインスタンスが１つのデータファイルに関連した位置に格納された関連情報を有するデータファイルにアクセスを試みる時を確認し、さらに前記管理プログラムが、前記格納された関連情報が現在アクセスを試みるソフトウエアのインスタンスに関連する情報であることを確認するシステム。

【請求項１８】　請求項１６において、前記管理プログラムが偽造できないハッシュ関数を使用して、現在アクセスを試みているデータファイルに関連する位置に格納された関連情報を確認するシステム。

【請求項１９】　請求項１において、保護センターが、タグ付けされたソフトウエアデータベースと、確認プログラムとを含み、

前記保護センターが呼び出し手順によって定期的にユーザー装置と通信してユーザー装置からタグを受け取り、前記タグはユーザー装置で使用されるタグ付けされたソフトウエアのインスタンスに関連付けされ、前記確認プログラムがタグ付けされたソフトウエアデータベースと対照してユーザー装置から受け取った各タグを検査して、タグが少なくとも１つの使用管理ポリシーに適合していることを保証し、さらに前記確認プログラムがユーザー装置に継続メッセージを返し、その継続メッセージが、ユーザー装置上の各タグに関連したソフトウエアのインスタンスに対してその後の動作を指示するものであり、

ユーザー装置上の前記管理プログラムが前記継続メッセージの認証を確認し、認証した場合は前記継続メッセージ内に指示されたその後の動作を実行するシステム。

【請求項２０】　請求項１９において、ソフトウエアベンダー、タグサーバーおよび保護センターの少なくとも１つが、ソフトウエアベンダー、タグサーバーおよび保護センターの内の少なくとも１つの他のものと結合されているシステム。

【請求項２１】　請求項１９において、連続した呼び出し手順間の最大許容

時間間隔が、ユーザー装置内で経過した時間、ユーザー装置が起動された回数、およびユーザー装置の使用程度の組合せの少なくとも１つにより決定されているシステム。

【請求項２２】　請求項２１において、最後の呼び出し手順後の前記最大許容時間間隔の終了以前に、ユーザー装置が前記保護センターによる呼び出し手順の実行に失敗したときは、そのユーザー装置が一定の期間無効にされるシステム。

【請求項２３】　請求項２１において、最後の呼び出し手順後の前記最大許容時間間隔の終了以前に、ユーザー装置が前記保護センターによる呼び出し手順の実行に失敗したときは、特定のソフトウエアのインスタンスの使用が一定の期間拒絶されるシステム。

【請求項２４】　請求項１９において、呼び出しが発生するのが、ソフトウエアのインスタンスがユーザー装置上で最初に使用される時であるシステム。

【請求項２５】　請求項１９において、呼び出しが発生するのが、前記保護センターからの要求によるものであるシステム。

【請求項２６】　請求項１９において、前記継続メッセージ内のタグテーブルのハッシュ関数値が、ユーザー装置からの呼び出しメッセージ内で送られたタグテーブル内のハッシュ関数値と同一であることを確認することにより、前記管理プログラムが継続メッセージの認証をテストするシステム。

【請求項２７】　請求項２６において、前記管理プログラムが、継続メッセージ内のデジタル署名が前記保護センターにより作成されたことを確認することにより、前記継続メッセージの認証がテストされるシステム。

【請求項２８】　請求項１９において、前記保護センターに対する呼び出しメッセージの後に続く継続メッセージを受信しないユーザー装置は、前の呼び出しメッセージに対するキャンセルコマンドを用いて呼び出しメッセージを再送信するシステム。

【請求項２９】　請求項１９において、少なくとも１つの使用管理ポリシーが、少なくとも１つのタグに関連付けされた少なくとも１つの個々のソフトウエアのインスタンスに関連付けされているシステム。

【請求項３０】　請求項１９において、少なくとも１つの使用管理ポリシーが、呼び出し手順中に保護センターが通信する全体のユーザー装置に関連付けされているシステム。

【請求項３１】　請求項１９において、少なくとも１つの使用管理ポリシーが、呼び出し手順の間に保護センターが通信するユーザー装置の個々のユーザーに関連付けされているシステム。

【請求項３２】　請求項１９において、少なくとも１つの使用管理ポリシーが、呼び出し手順中に保護センターが通信するユーザー装置の使用履歴に関連付けされているシステム。

【請求項３３】　請求項１９において、前記保護センターが、各ユーザー装置上の各ソフトウエアのインスタンスの関連する各タグに対する、タグ付けされたソフトウエアデータベースのタグデータ構造体を保持するシステム。

【請求項３４】　請求項３３において、各タグデータ構造体がソフトウエアのインスタンスのタグと、前記ソフトウエアのインスタンスに関連する使用管理ポリシーと、呼び出し記録に対する参照の収集物とを含むシステム。

【請求項３５】　請求項３４において、呼び出し記録の前記収集物内の各呼び出し記録が、１つの呼び出し手順に関する情報を表し、また前記呼び出し手順に関連する継続メッセージが、少なくとも１つの呼び出し時刻と、呼び出し手順の間に保護センターに転送されるタグテーブルのヘッダーと、前の呼び出し手順の時刻表示を示す最後の呼び出し時刻と、呼び出し手順の間に保護センターに転送される前記タグテーブルのハッシュ関数値と、ユーザー装置のその後の動作とを含むシステム。

【請求項３６】　請求項１において、確認プログラムを含む保護センターをさらに備え、

前記保護センターが呼び出し手順によってユーザー装置と定期的に通信して、そのユーザー装置からユーザー装置管理プログラムに対する固有の識別子を受け取り、前記確認プログラムが前記固有の識別子をテストして、多くても１つの管理プログラムがその識別子を有し、前記確認プログラムがユーザー装置に継続メッセージを返し、ユーザー装置上の各タグに関連するソフトウエアのインスタン

スの使用を試みる際に前記継続メッセージがその後の動作を指示し、

前記ユーザー装置の管理プログラムが継続メッセージの認証を確認し、認証された場合は、その継続メッセージ内の動作を実行するシステム。

【請求項３７】　請求項３６において、前記管理プログラムが呼び出される最初の時に、まれにしか複製されない番号に基づいて、前記管理プログラム識別子が作成されるシステム。

【請求項３８】　請求項３７において、前記まれにしか複製されない番号は、前記管理プログラムが装置により最初に呼び出される時に発生する非常に正確なクロック値であるシステム。

【請求項３９】　請求項３７において、前記まれにしか複製されない事象が、保護センターにより提供される番号であるシステム。

【請求項４０】　請求項１において、ユーザー装置上で使用されるタグ付けされていないソフトウエアのインスタンスをさらに備え、

前記管理プログラムが前記タグ付けされていないソフトウエアのインスタンスを検出して、前記タグ付けされていないソフトウエアのインスタンス上の指紋処理を実行し、ユーザー装置上の前記指紋処理の結果である指紋を格納するシステム。

【請求項４１】　請求項４０において、前記ユーザー装置の管理プログラムが、前記装置上で使用されるタグ付けされていないソフトウエアのインスタンス上の指紋処理をさらに実行し、前記ユーザー装置上の指紋テーブル内の指紋処理から得られる前記指紋を格納するシステム。

【請求項４２】　請求項４１において、前記管理プログラムが指紋を計算した位置を格納するシステム。

【請求項４３】　請求項４１において、前記指紋が前記ソフトウエアのインスタンスの内容に基づくシステム。

【請求項４４】　請求項４１において、前記指紋が前記ソフトウエアのインスタンスの挙動の既知のシーケンスに基づくシステム。

【請求項４５】　請求項４１において、指紋データ構造体と確認プログラムを含む保護センターをさらに備え、

前記保護センターが呼び出し手順によってユーザー装置と定期的に通信して、前記ユーザー装置上で使用されるソフトウエアのインスタンスに対するユーザー装置からの全指紋を受け取り、前記確認プログラムが前記指紋データ構造体に対してユーザー装置から受け取ったすべての指紋を比較し、ユーザー装置上で使用されるソフトウエアのインスタンスが権利侵害のソフトウエアのインスタンスであるかどうかを決定するシステム。

【請求項４６】　請求項４５において、前記確認プログラムが、前記保護センターの指紋データ構造体内の指紋とユーザー装置から受け取った指紋との間の一致の指定数より多くの一致を検出した場合は、前記確認プログラムが実行すべき報復措置を指定して、継続メッセージをユーザー装置に返し、前記継続メッセージが前記ユーザー装置上で実行すべき報復措置を指示するシステム。

【請求項４７】　請求項４６において、前記指紋一致処理が少なくとも１つの一般位置または同一位置指紋一致であるシステム。

【請求項４８】　請求項４６において、前記指紋一致が反転保護センター指紋テーブルを使用するシステム。

【請求項４９】　請求項４６において、前記報復措置が、ユーザー装置を指定時間無効にすることを指定するシステム。

【請求項５０】　請求項４６において、前記報復措置が、保護センターの指紋データ構造体内の指紋に一致した指紋に関連するソフトウエアのインスタンスを指定時間無効にすることを指定するシステム。

【請求項５１】　請求項４６において、前記報復措置が、ユーザー装置の挙動履歴と、ユーザー装置上の特定ユーザーの挙動履歴と、ユーザー装置上の他のソフトウエアの収集物との組み合わせの少なくとも１つに依存しているシステム。

【請求項５２】　請求項４５において、前記ソフトウエアベンダーが権利侵害のソフトウエアインスタンスのコピーを保護センターに送信し、前記保護センターが前記権利侵害のソフトウエアインスタンス上の指紋を計算し、さらに保護センター上の指紋データ構造体内に前記指紋を格納するシステム。

【請求項５３】　ユーザー装置の読み取り可能媒体上で符号化されたタグテ

ーブルデータ構造体であって、前記タグテーブルデータ構造体が、１つのソフトウエアインスタンスに一意的に関連付けされた少なくとも１つのタグを含み、タグテーブル内の前記タグに関連する少なくとも１つの領域を含み、さらにソフトウエアインスタンスに関連する前記タグに関連する使用状況を表す少なくとも１つの領域を含んでいるタグテーブルデータ構造体。

【請求項５４】　請求項５３において、前記少なくとも１つの領域が、タグに関連する前記１つのソフトウエアインスタンスに対する使用統計を表しているタグテーブルデータ構造体。

【請求項５５】　請求項５３において、前記タグテーブルを一意的に識別するタグテーブルヘッダをさらに含んでいるタグテーブルデータ構造体。

【請求項５６】　請求項５３において、前記タグテーブルヘッダがユーザー装置使用統計に関する情報と継続メッセージを含んでいるタグテーブルデータ構造体。

【請求項５７】　それぞれが少なくとも１つの名称とソフトウエア内容を有する、ソフトウエアインスタンスを作成するソフトウエア作成機構と、

各ソフトウエアインスタンスがそのソフトウエアインスタンスに固有のタグだけに関連して使用でき、また前記タグが、そのタグに関連付けされた前記ソフトウエアインスタンスに関連する情報の固有の偽造できない収集物であり、さらに前記ソフトウエアの少なくとも１つの名称と、前記ソフトウエアインスタンスの固有の番号と、前記ソフトウエア内容の各部分のハッシュ関数値を含むソフトウエアインスタンスとを備えているソフトウエアベンダー。

【請求項５８】　請求項５７において、前記タグが、ソフトウエアインスタンスを使用するユーザー装置に関連する前記管理プログラムの識別子を含んでいるソフトウエアベンダー。

【請求項５９】　請求項５７において、前記タグが、前記タグが関連付けされているソフトウエアインスタンスの各部分の指紋のリストを含んでいるソフトウエアベンダー。

【請求項６０】　請求項５７において、ベンダーの権利を侵害するソフトウエアを検出し、その権利侵害のソフトウエアのコピーを保護センターに転送して

使用管理を実行し、ユーザー装置上の権利侵害のソフトウエアインスタンスの使用を検出できるようにする権利侵害ソフトウエア検出機構を備えているソフトウエアベンダー。

【請求項６１】　請求項６０において、ベンダーの権利を侵害するソフトウエアを検出し、その権利侵害のソフトウエアのコピーを保護センターに転送し、前記保護センターが前記権利侵害のソフトウエアインスタンスに関連するすべてのタグを無効にし、前記権利侵害のソフトウエアインスタンスを使用した保護センターにより検出されたすべてのユーザー装置に対し報復措置を送信する権利侵害ソフトウエア検出機構を備えているソフトウエアベンダー。

【請求項６２】　ソフトウエアインスタンスと、一意的に関連付けされたタグと、ソフトウエアインスタンスを使用するための要求とを受け取る入力ポートと、

管理プログラムを実行するプロセッサであって、前記ソフトウエアインスタンス使用するための要求を検出し、ソフトウエアインスタンスに関連するタグの認証を確認した後、ユーザー装置での前記ソフトウエアインスタンスの使用を許可するプロセッサとを備えているユーザー装置。

【請求項６３】　請求項６２において、前記管理プログラムが、前記タグの認証を確認し、タグテーブル内にそのタグを保持し、そのタグが認証されている場合は前記ソフトウエアインスタンスを維持し、ソフトウエアに関連する前記タグが認証されていない場合は前記ソフトウエアインスタンスを拒絶するユーザー装置。

【請求項６４】　請求項６３において、前記管理プログラムが、前記ソフトウエアインスタント上のハッシュ関数値を計算し、その計算した値を前記タグ内のハッシュ関数値と比較して、前記タグが認証されているかどうか、さらに前記ソフトウエアインスタンスに適正に関連付けされているかどうかを決定するユーザー装置。

【請求項６５】　請求項６３において、前記タグがディジタル的に署名され、前記管理プログラムがタグのディジタル署名を確認することによりタグの認証を確認するユーザー装置。

【請求項６６】　請求項６３において、前記タグテーブルがユーザー装置上のストレージ内に格納されたデータ構造体であり、ソフトウエアインスタンスに一意的に関連する少なくとも１つのタグを含み、さらにタグテーブル内の前記タグに関連する少なくとも１つの領域を含むものであって、前記少なくとも１つの領域が前記タグに関連する前記ソフトウエアインスタンスに対する使用状況を表しているユーザー装置。

【請求項６７】　請求項６２において、前記管理プログラムが、呼び出しポリシーによる規定にしたがって呼び出し手順を要求することを決定し、さらに前記管理プログラムが、前記呼び出し手順を実行してタグテーブル内に格納されたタグの前記使用状況を更新するユーザー装置。

【請求項６８】　請求項６２において、前記管理プログラムが、タグ付けされたソフトウエアで使用される各データが正当なソフトウエアインタンスにより作成されていることを確認するユーザー装置。

【請求項６９】　請求項６７において、前記呼び出し手順の実行中に、前記管理プログラムがユーザー装置に接続された相互接続機構を介してユーザー装置から前記タグテーブルを安全に送信し、前記ユーザー装置に返送される継続メッセージの受け取りを待機するものであり、前記継続メッセージが前記タグテーブル内の各タグに対し実行すべき動作を指示しているユーザー装置。

【請求項７０】　請求項６７において、前記呼び出し手順の実行中に、前記管理プログラムが、ユーザー装置に接続された相互接続機構を介してユーザー装置からタグテーブルヘッダを安全に送信し、前記ユーザー装置に返送される、前記タグテーブル内の各タグに対し実行すべき動作を指示している継続メッセージの受け取りを待機するユーザー装置。

【請求項７１】　請求項６２において、前記ユーザー装置上で使用されるタグ付けされていないソフトウエアインスタンスをさらに備え、

前記管理プログラムが、前記タグ付けされていないソフトウエアインスタンスを検出して、前記タグ付けされていないソフトウエアインスタンス上の指紋処理を実行し、前記ユーザー装置上の指紋テーブル内の前記指紋処理から得た指紋を格納するユーザー装置。

【請求項７２】　請求項７１において、前記管理プログラムが、呼び出しポリシーによる規定にしたがって呼び出し手順を要求することを決定し、さらに前記管理プログラムが、前記呼び出し手順を実行して、ユーザー装置に格納されたタグ付けされていないソフトウエアインスタンスの使用状況を更新するユーザー装置。

【請求項７３】　請求項７２において、前記呼び出し手順の実行中に、前記管理プログラムが、ユーザー装置に接続された相互接続機構を介して前記ユーザー装置から前記指紋テーブルの一部を送信し、さらに前記ユーザー装置に返送される、前記ユーザー装置に格納された各タグ付けされていないソフトウエアインスタンスに対し実行すべき動作を指示する継続メッセージの受け取りを待機するユーザー装置。

【請求項７４】　タグ付けされたソフトウエアデータベースと、内部のプロセッサで実行する確認プログラムとを備える保護センターであって、

前記保護センターが、呼び出し手順を定期的に実行し、相互接続を介して、ソフトウエアインスタンスに対するタグを受け取るものであって、前記確認プログラムが、保護センターに保持されている前記タグ付けされたソフトウエアデータベースに対して受け取ったタグを検査し、前記タグが少なくとも１つの使用管理ポリシーに適合していることを確認し、さらに前記管理プログラムが、相互接続機構を介して、前記呼び出し手順の間に保護センターで受け取られた各タグに関連するソフトウエアインスタンスの使用時にしたがうべき動作を指示している継続メッセージを送信する保護センター。

【請求項７５】　請求項７４において、少なくとも１つの使用管理ポリシーが、少なくとも１つのタグが関連付けされている各ソフトウエアインスタンスに関連付けされている保護センター。

【請求項７６】　請求項７４において、少なくとも１つの使用管理ポリシーが、前記保護センターがタグを受け取るために通信するユーザー装置に関連付けされている保護センター。

【請求項７７】　請求項７４において、少なくとも１つの使用管理ポリシーが、前記保護センターがタグを受け取る目的で通信するユーザー装置の個々のユ

ーザーに関連付けされている保護センター。

【請求項７８】　請求項７４において、前記タグ付けされたソフトウエアデータベース内に、各ユーザー装置上の各ソフトウエアインスタンスに関連する各タグに対するタグデータ構造体を保持し、またタグサーバからのソフトウエアインスタンスに関連する新しく作成されたタグを受信し、さらにユーザー装置から送信されたタグテーブル内のユーザー装置で使用されるソフトウエアインスタンスに関連するタグを受信する保護センター。

【請求項７９】　請求項７８において、各タグデータ構造体が、ソフトウエアインスタンスの少なくとも１つのタグと、ソフトウエアインスタンスの名称と、前記ソフトウエアインスタンスの固有の番号と、前記ソフトウエアインスタンスのハッシュ関数値と、前記ソフトウエアインスタンスの使用管理ポリシーと、前記ソフトウエアインスタンスに関連するタグに関連付けされた呼び出しレコードへの参照の収集物とを含んでいる保護センター。

【請求項８０】　請求項７９において、呼び出しレコードの前記収集物内の各呼び出しレコードが１つの呼び出し手順に関する情報を表し、さらに前記各呼び出しレコードが少なくとも１つの呼び出し時刻と、前記呼び出し手順の間に保護センターに転送されるタグテーブルのヘッダーと、前の呼び出し手順の時刻表示を示す最後の呼び出し時刻と、前記呼び出し手順の間に保護センターに転送される前記タグテーブルのハッシュ関数値と、前記呼び出し手順に関連する継続メッセージ内に含まれるユーザー装置のその後の動作とを含む保護センター。

【請求項８１】　指紋データ構造体と、確認プログラムを実行するプロセッサとを含む保護センターであって、

前記確認プログラムが、ユーザー装置を用いて呼び出し手順を定期的に実行し、相互接続機構を介して、前記ユーザー装置で使用されるソフトウエアインスタンスに対する指紋を受信し、さらに前記確認プログラムが、指紋データ構造体に対して受け取った各指紋を検査し、ユーザー装置で使用されるタグ付けされていないソフトウエアインスタンスが権利侵害のソフトウエアインスタンスであるかどうかを決定し、権利侵害している場合は、前記確認プログラムが、前記ユーザー装置で実行される報復措置を準備する保護センター。

【請求項８２】　請求項８１において、すべてのベンダーソフトウエアが指紋付けされ、別のベンダーソフトウエアに関する１つのベンダーソフトウエアの権利侵害が、少なくとも１つの同一位置または一般位置の指紋検査に基づいて検出される保護センター。

【請求項８３】　請求項８１において、前記確認プログラムが、指紋データ構造体内の指紋と受け取った指紋内の指紋の間の十分な数の一致を検出する場合は、前記確認プログラムが実行すべき報復措置を指定して、継続メッセージを送信するものであり、前記継続メッセージがそのメッセージの受信機で実行される報復措置を指示している保護センター。

【請求項８４】　請求項８３において、前記十分な数が１つである保護センター。

【請求項８５】　請求項８３において、前記十分な数が１よりも大きい保護センター。

【請求項８６】　請求項８５において、前記十分な数が、各一致の重みが一致する指紋に依存する場合の、一致の重み付けされた総和として計算される保護センター。

【請求項８７】　請求項８３において、前記指紋照合法が一般位置の指紋検査である保護センター。

【請求項８８】　請求項８３において、前記報復措置が受信機の実行停止を指定する保護センター。

【請求項８９】　請求項８３において、前記報復措置が、前記指紋データ構造体内の指紋に一致した指紋に関連したソフトウエアインスタンスを無効にすることを、指定する保護センター。

【請求項９０】　請求項８１において、前記確認プログラムが、相互接続機構を介して、権利侵害のソフトウエアインスタンスのコピーを受け取り、さらに前記タグ付けされていない権利侵害のソフトウエアインスタンスのコピー上の指紋を計算し、前記指紋を前記指紋データ構造体内に組み込んで格納する保護センター。

【請求項９１】　特定ベンダーのソフトウエアのコピーを受け取り、前記ソ

フトウエアインスタンスあたり複数タグを作成するタグサーバにおいて、

各タグがそのタグに関連付けられたソフトウエアインスタンスを一意的に識別し、さらに各タグが前記タグに関連する前記ソフトウエアの少なくとも１つの名称と、前記タグに関連する前記ソフトウエアインスタンスの固有の番号と、前記タグに関連する前記ソフトウエアインスタンスの各部分で計算されたハッシュ関数値とを含んでいるタグサーバ。

【請求項９２】　請求項９１において、前記タグにデジタル的に署名し、そのタグを、意図する受信機に安全に送信するために使用されるデジタル署名機構をさらに含んでいるタグサーバ。

【請求項９３】　ソフトウエアインスタスを作成するステップと、

前記ソフトウエアインスタスに一意的に関連付けされたタグを作成するステップと、

前記ソフトウエアインスタスを配信し、前記タグをユーザー装置に安全に配信し、前記ソフトウエアインスタンスと前記関連するタグを前記ユーザー装置で受け取るステップと、

前記ユーザー装置上での前記ソフトウエアインスタンスの使用を検出するステップと、

使用される前記ソフトウエアインスタンスに関連している前記タグのステータスを判定することにより、前記ソフトウエアインスタンスの使用が可能かどうかを決定するステップとを含んでいるソフトウエアの使用を管理するための方法。

【請求項９４】　請求項９３において、前記タグを作成するステップが、

前記ソフトウエアインスタンスに固有の番号を割り当てるステップと、

前記ソフトウエアインスタンスの内容の各部の第１ハッシュ関数値を計算するステップと、

前記ソフトウエアインスタンスに対し第２ハッシュ関数値を計算するステップであって、前記第２ハッシュ関数値がソフトウエアの前記名称と、前記ソフトウエアインスタンスに固有の番号と、第１ハッシュ関数値とを組み合わせている、第２ハッシュ関数値を計算するステップと、

前記ソフトウエアインスタンスに一意的に関連付けられるタグを計算するステ

ップであって、前記タグがソフトウエアの前記名称と、前記ソフトウエアインスタンスの固有の番号と、第２ハッシュ関数値とを含む、タグを計算するステップとを含んでいる方法。

【請求項９５】　請求項９４において、前記タグを計算するステップが、前記第２ハッシュ関数に対してデジタル署名関数を適用し、前記タグ内に前記署名を含むことによりデジタル的に署名されたタグを作成する方法。

【請求項９６】　請求項９３において、前記タグをユーザーに配信するステップが、前記タグをソフトウエアベンダーに安全に配信するステップを含み、ユーザー装置が公開鍵暗号化方式を使用する方法。

【請求項９７】　請求項９３において、前記ソフトウエアインスタンスを受け取るステップが、前記ユーザー装置で前記ソフトウエアインスタンスを受け取るステップを含み、

前記ユーザー装置でタグを受け取るステップが、

前記ユーザー装置でソフトウエアインスタンスに関連する前記タグを安全に受け取るステップと、

前記ソフトウエアインスタンスに関連する前記タグが署名されているかどうかを決定し、署名されていれば、前記タグ内のハッシュ関数値の署名を確認して、ユーザー装置に前記ソフトウエアをインストールし、また前記ソフトウエアインスタンスに関連する前記タグが署名されていない場合は、ユーザー装置に前記ソフトウエアインスタンスをインストールするステップとを含んでいる方法。

【請求項９８】　請求項９３において、前記ユーザー装置での前記ソフトウエアインスタンスの使用を検出するステップが、

前記ユーザー装置上の管理プログラムを呼び出して、前記ソフトウエアインスタンスの使用に対するユーザー要求を遮断するステップを含み、

前記ソフトウエアインスタンスの使用を可能にするかどうかの決定のステップが、

呼び出しポリシーに基づいて呼び出し手順が必要かどうかを決定し、必要なら次の３つのステップ、

１）呼び出し手順を実行し、認証を確認して、ソフトウエアインスタンスに

関連するタグの前記使用管理ポリシーを決定するステップと、

２）前記呼び出し手順の結果に基づいて前記ユーザー装置内の情報を更新するステップと、

３）前記タグに関連するステータス情報を検査して、前記タグに関連するソフトウエアインスタンスの使用が可能かどうかを決定するステップとを実行する方法。

【請求項９９】　請求項９８において、前記呼び出し手順を実行するステップが、

ユーザー装置から前記ソフトウエアインスタンスに関連する前記タグを格納しているタグテーブルを送信するステップと、

ユーザー装置から返送された、前記タグテーブル内の各タグに対し実行される動作を指示する継続メッセージの受信を待機するステップとを含んでいる方法。

【請求項１００】　請求項９８において、前記継続メッセージがこの装置方向に向けられ、また事象履歴がこの装置の事象履歴に一致することを確認するステップをさらに含んでいる方法。

【請求項１０１】　請求項９８において、前記呼び出し手順を実行するステップが、

ソフトウエアインスタンスに関連する前記タグを含むタグテーブルを受け取るステップと、

前記タグテーブル内の受け取った各タグをタグ付けされたソフトウエアデータベースに対して検査して、前記タグテーブル内のタグが少なくとも１つの使用管理ポリシーに適合していることを確認するステップと、

各タグに関連する前記ソフトウエアインスタンスの使用を検出した時点で、前記ユーザー装置でその後に実行する動作を指示する継続メッセージを送信するステップとを含む方法。

【請求項１０２】　請求項１０１において、前記継続メッセージが、

前記継続メッセージを送信する宛先の前記管理プログラムの管理プログラム識別子と、

前記継続メッセージが準備された時刻と、

前記装置からの前記呼び出しに付随しているタグテーブルの符号化とを含んでいる方法。

【請求項１０３】　ユーザー装置上のタグ付けされていないソフトウエアインスタンスの使用を検出するステップと、

ユーザー装置上の前記タグ付けされていないソフトウエアインスタンスに関連する指紋を作成して格納するステップと、

ユーザー装置上の前記タグ付けされていないソフトウエアインスタンスの使用を検出するステップと、

前記タグ付けされていないソフトウエアインスタンスに関連する指紋と権利侵害の指紋の指紋データ構造体とを比較して、前記ソフトウエアインスタンスの使用が正当であるかどうかを決定し、指紋の一致が発見されると前記タグ付けされていないソフトウエアインスタンスの使用を無効とするステップとを含んでいるソフトウエアの使用を管理するための方法。

【請求項１０４】　請求項１０３において、ユーザー装置上のタグ付けされたソフトウエアインスタンスの使用を検出するステップと、

ユーザー装置上の前記タグ付けされたソフトウエアインスタンスに関連する指紋を作成して格納するステップと、

ユーザー装置上の前記タグ付けされたソフトウエアインスタンスの使用を検出するステップと、

前記タグ付けされたソフトウエアインスタンスに関連する指紋と権利侵害の指紋の指紋データ構造体とを比較して、前記ソフトウエアインスタンスの使用が正当であるかどうかを決定し、指紋の一致が発見されると前記タグ付けされたソフトウエアインスタンスの使用を無効とするステップとをさらに含んでいる方法。

【請求項１０５】　請求項１０３において、ソフトウエアベンダーにより、権利侵害のソフトウエアインスタンスを検出するステップと、

前記権利侵害のソフトウエアインスタンスのコピーを保護センターに提出するステップと、

前記保護センターにおいて、権利侵害のソフトウエアインスタンス上の指紋を計算し、指紋データ構造体内にその指紋を組み込んで格納するステップとをさら

に含んでいる方法。

【請求項１０６】　ソフトウエアインスタンスを取得するステップと、

前記ソフトウエアインスタンスに名称を割り当てるステップと、

前記ソフトウエアインスタンスに、同一ソフトウエアの別のインスタンスに割り当てられるすべての固有番号と異なる固有番号を割り当てるステップと、

前記ソフトウエアインスタンスの各部分のハッシュ関数値を計算するステップと、

ソフトウエアインスタンスの前記名称と、前記ソフトウエアインスタンスの番号と、最初に計算されたハッシュ関数値との連続に関する第２ハッシュ関数値を計算して、そのソフトウエアインスタンスに固有の署名のないハッシュ関数値を作成するステップと、

鍵を使用して前記署名のないハッシュ関数値に署名して、前記ソフトウエアインスタンスに対する署名されたハッシュ関数を作成するステップと、

そのソフトウエアインスタンスを一意的に識別する前記ソフトウエアインスタンスに関連付けされたタグを作成するステップであって、前記タグがソフトウエアインスタンスの前記署名されたハッシュ関数と、ソフトウエアインスタンスの前記名称と、ソフトウエアインスタンスの前記固有番号と、ソフトウエアインスタンスの前記署名のないハッシュ関数とを含む、タグを作成するステップとを含む、ソフトウエアインスタンスを一意的に識別するための方法。

【請求項１０７】　請求項１０６において、前記ソフトウエアインスタンスを取得するステップと、そのソフトウエアに名称を割り当てるステップとがソフトウエアベンダーによって実行され、また前記ソフトウエアインスタンスに固有番号を割り当てるステップと、前記第１および第２ハッシュ関数値を計算するステップと、前記第２ハッシュ関数値に著名するステップと、前記タグを作成するステップとがタグサーバーにより実行される方法。

【請求項１０８】　命令によって符号化されたコンピューター読み取り可能媒体であって、プロセッサで読み取りおよび実行されるときに、ソフトウエアインスタンスを使用する要求を検出するステップを実行し、

そのステップでは、前記ソフトウエアインスタンスに対応するタグが、前記ソ

フトウエアの使用を認める関連ステータスを有するかどうか決定し、定期的に呼び出し手順を実行して前記タグの認証を確認し、前記タグに対応する前記ソフトウエアインスタンスが使用管理ポリシーにしたがって使用されることを確認するコンピューター読み取り可能媒体。

【請求項１０９】　通信媒体上を搬送波によって伝送される伝播信号であって、

前記信号が、１つのソフトウエアインスタンスに一意的に関連付けされた少なくとも１つのタグを含み、かつタグテーブル内の前記タグに関連する少なくとも１つの領域を含む符号化されたタグテーブルデータ構造体を有し、前記少なくとも１つの領域が前記タグに関連する１つのソフトウエアインスタンスに対する使用制御ステータスを表している伝播信号。

【請求項１１０】　媒体上を搬送波により伝送される伝播信号であって、前記信号が符号化された継続メッセージを有し、ある動作に関連するソフトウエアインスタンスの使用要求が受信機で検出されたとき、前記継続メッセージが前記伝播信号の受信機で実行される前記動作の指示を含む伝播信号。

【請求項１１１】　ソフトウエアプログラムの内容に関し偽造できないハッシュ関数値を計算するステップと、

前記偽造できないハッシュ関数の前記結果を前に保持されたハッシュ関数値と比較してその結果が同一かどうかを決定し、それによりソフトウエアが変更していないかどうかを示すステップとを含んでいるソフトウエアプログラムが変化していないことを確認する方法。

【請求項１１２】　請求項１１１において、前記オペレーティングシステムが前記偽造できないハッシュ関数値を計算し、前記ソフトウエアプログラムが前記管理プログラムである方法。

【請求項１１３】　データの内容に関する偽造できないハッシュ関数値を計算して、その値を前に計算したハッシュ関数値と比較することにより、データが変化していないことを確認する方法。

【請求項１１４】　請求項１１３において、前記管理プログラムが、前記偽造できないハッシュ関数値と、前記管理プログラムで使用される前記データとを

計算する方法。

【請求項１１５】　請求項１９において、前記保護センターとユーザー装置間の全メッセージが安全な方法で送信されるシステム。

【請求項１１６】　請求項１１５において、前記安全な方法が公開鍵暗号化方式を含むシステム。

【請求項１１７】　請求項３８において、さらに、前記まれにしか複製されない数が少なくとも１つのメモリ位置の値に基づいているシステム。

【請求項１１８】　請求項８０の保護センターにおいて、前記装置からの前記継続メッセージ内に記録された最後の呼び出し時刻が、この装置に対する前記保護センターに記録された最新呼び出しの呼び出し時刻に一致するかどうかを検査する保護センター。

【請求項１１９】　ソフトウエアの使用を管理するためのシステムであって、

ソフトウエアインスタンスを作成するソフトウエアベンダーと、

ソフトウエアインスタンスを受け取ってそれをインストールするユーザー装置であって、かつ管理プログラムを含むユーザー装置と、

前記ユーザー装置上で使用されるタグ付けされていないソフトウエアインスタンスとを含み、

前記管理プログラムが、前記タグ付けされていないソフトウエアインスタンスの使用を検出し、前記タグ付けされていないソフトウエアインスタンス上の指紋処理を実行し、前記ユーザー装置上の指紋処理から得た指紋を格納するシステム。

【請求項１２０】　請求項１１９において、前記ユーザー装置の管理プログラムが、前記装置上でタグ付けされていないソフトウエアインスタンスの指紋処理を実行し、前記ユーザー装置上の指紋テーブル内に前記指紋処理から得た指紋を格納するシステム。

【請求項１２１】　請求項１２０において、前記管理プログラムが指紋を計算する位置を格納するシステム。

【請求項１２２】　請求項１２０において、前記指紋がソフトウエアインス

タンスの内容に基づいているシステム。

【請求項１２３】　請求項１２０において、前記指紋がソフトウエアインスタンスの挙動の既知のシーケンスに基づいているシステム。

【請求項１２４】　請求項１２０において、前記保護センターが、指紋データ構造体と確認プログラムとをさらに含み、

前記保護センターが呼び出し手順によってユーザー装置と定期的に通信して、前記ユーザー装置で使用されるソフトウエアインスタンスに対するユーザー装置からの全指紋を受け取り、前記管理プログラムが前記ユーザー装置から受け取ったすべての指紋を指紋データ構造体に対して比較して、前記ユーザー装置で使用されるソフトウエアインスタンスが権利侵害のソフトウエアインスタンスかどうかを決定するシステム。

【請求項１２５】　請求項１２４において、前記管理プログラムが、保護センターの指紋データ構造体内の指紋とユーザー装置から受け取った指紋との一致の特定数より多くの一致がある場合は、前記管理プログラムが実行すべき報復措置を指定し、さらに前記ユーザー装置に継続メッセージを返送するものであり、前記継続メッセージが前記ユーザー装置で実行される前記報復措置を指定するシステム。

【請求項１２６】　請求項１２５において、前記指紋一致プロセスが少なくとも１つの一般位置または同一位置の指紋一致であるシステム。

【請求項１２７】　請求項１２５において、前記指紋一致が反転保護センター指紋テーブルを使用するシステム。

【請求項１２８】　請求項１２５において、前記報復措置が、ユーザー装置を特定時間無効にすることを指定するシステム。

【請求項１２９】　請求項１２５において、前記報復措置が、保護センターの指紋データ構造体内の指紋に一致した指紋に関連する前記ソフトウエアインスタンスを特定時間無効にすることを指定するシステム。

【請求項１３０】　請求項１２５において、前記報復措置が、ユーザー装置の動作履歴と、前記ユーザー装置上の特定ユーザーの動作履歴と、前記ユーザー装置上の他のソフトウエアの収集物の組合せの少なくとも１つに依存しているシ

ステム。

【請求項１３１】　請求項１２４において、前記ソフトウエアベンダーが権利侵害のソフトウエアインスタンスのコピーを保護センターに送信し、前記保護センターが前記権利侵害のソフトウエアインスタンスのコピーの指紋を計算し、さらに保護センター上の指紋データ構造体内に前記指紋を格納するシステム。

【請求項１３２】　装置識別子を検査内に組み込んだ少なくとも１つのソフトウエアインスタンスを作成するソフトウエア作成機構と、

前記ソフトウエアインスタンスを受け取ってインストールするユーザー装置とを含むソフトウエアベンダーであって、

前記検査が、前記組み込まれた識別子と前記ソフトウエアインスタンスを使用する装置の識別子との比較を含み、

前記組み込まれた識別子が前記装置の識別子に等しい場合は、前記ソフトウエアインスタンスを使用でき、等しくない場合は前記装置上の管理プログラムにより報復措置を実行するソフトウエアベンダー。

【請求項１３３】　請求項１３２において、前記ソフトウエアベンダーが前記ソフトウエアインスタンスのハッシュのデジタル署名を送信し、

第２試験が前記デジタル署名が認証できるかどうかを決定し、

第３試験が前記署名された値が前記ソフトウエアインスタンスのハッシュに等しいかどうかを決定するものであって、

前記デジタル署名が認証できないかまたは署名された値が前記ソフトウエアインスタンスと異なる場合は、前記装置の管理プログラムが報復措置を実行するソフトウエアベンダー。

【請求項１３４】　請求項１３１において、前記装置識別子が前記ソフトウエアインスタンスの内容の最初の部分または最後の部分に組み込まれているソフトウエアベンダー。

【請求項１３５】　ソフトウエアの使用を管理するための方法であって、

装置識別子を検査内に組み込んだソフトウエアインスタンスを作成するステップであって、　前記検査が、前記組み込まれた識別子と前記ソフトウエアインスタンスを使用する装置の識別子との比較を含むステップと、

前記ソフトウエアインスタンスをユーザー装置に配布するステップと、

前記検査を実行することにより前記ソフトウエアインスタンスの使用が可能かどうかを決定して、前記組み込まれた識別子が前記装置の識別子に等しい場合は前記ソフトウエアインスタンスを使用できるように使用を許可し、等しくない場合は報復措置を実行するステップとを含んでいる方法。

【請求項１３６】　請求項１３５において、前記ソフトウエアインスタンスの前記ハッシュのデジタル署名を送信するステップと、

前記デジタル署名が認証できるかどうかを決定するステップと、

前記署名された値が前記ソフトウエアインスタンスの前記ハッシュに等しいかどうかを決定するステップとを含み、

前記デジタル署名が認証できないかまたは署名された値が前記ソフトウエアインスタンスと異なる場合は、前記装置の管理プログラムが報復措置を実行する方法。

【請求項１３７】　請求項１３５において、前記装置識別子が前記ソフトウエアインスタンスの最初の部分または最後の部分に配置されている方法。

【発明の詳細な説明】

【０００１】

【発明の背景】

ソフトウエアもしくは情報の著作権侵害は、当該ソフトウエアもしくは情報の作成者または正当な所有者の許可を得ることなく、ソフトウエアもしくは情報を使用し、またはコピーする行為である。著作権侵害は、コンピュータソフトウエア産業分野において最も横行し、この分野ではソフトウエアアプリケーションの不正コピーが頻繁に行われている。アプリケーションは、私的な使用や、再生産、販売用にコピーされる。他のタイプの著作権侵害行為は、音楽の録音、ドキュメントの読み出し可能なバージョン、または電子ブックのような情報をコピーする行為を含む。著作権の侵害によるビジネスの逸失利益額は、年間に何十億ドルに達すると考えられる。

【０００２】

ソフトウエアおよび情報技術産業は、著作権侵害の脅威に対してロック方式の使用により対応してきた。ロック方式は、ソフトウエアロック機構、ライセンス、および特殊なハードウエア装置を有し、これがソフトウエア、情報、またはエレクトロニクス装置全体の不正使用を防止する。これらの方式は、不正使用者がソフトウエアを自由にコピーすることを阻止する。

【０００３】

ソフトウエアロック機構には多くのタイプがある。例えばメーカは、ソフトウエアプログラムの部分を鍵（キー）を用いて暗号化する。ソフトウエアを購入するユーザーには、ソフトウエアを解読し実行する鍵が与えられる。このようなソフトウエア保護機構の例は、マイクロソフト　ウィンドウズ（登録商標）９８のようなソフトウエアの購入時に供給される“真正証明”であり、マイクロソフトコーポレーション（レドモンド，ワシントン州）により製作されている。マイクロソフトおよびウィンドウズ９８は、マイクロソフト　コーポレーションの商標である。真正証明は、個他の製品番号を示す。ソフトウエアのインストール中、製品番号はソフトウエアアプリケーションにより要求され、ユーザーにより正しく入力される必要がある。入力された製品番号は、ソフトウエアアプリケーシ

ョンにより期待された番号に一致する時にアプリケーションのコピーは正当とされ、インストールされ、実行される。入力された番号が正しくなければソフトウエアは正しくインストールされないことになる。

【０００４】

ハードウエア著作権保護方式は、あるハードウエア装置をプロセッサに通信ポートを介して取り付ける。これらのタイプのハードウエア装置は、“ドングル”と呼ばれる。ハードウエア保護方式の例は、米国特許Ｎｏ．３，９９６，４４９に記載され、この特許ではコンピュータの作動中にプログラムまたはプログラムの一部が有効であるか否かを判断するための方法が開示されている。このシステムでは、ハッシュ関数が不正防止ハードウエアチェック装置のプログラムテキストと共にユーザー識別コードまたは鍵に用いられる。チェック装置は、プログラムテキストが正しいか否かを知るためにハッシュ関数から得られた値を確認値と比較する。テキストが正しければプログラムは装置で実行される。

【０００５】

他のハードウエア関連の方法は、プログラムを実行する各プロセッサに個々の識別子を割り当てる。これによりソフトウエアプログラムは、そのプログラムが割り当てられ、または実行が許可される指定プロセッサ識別子照合を用いて暗号化される。他のプロセッサの識別子は、ソフトウエアに存在せず、従ってソフトウエアは他のプロセッサで作動することはない。当然このようなシステムは、そのシステムが関連付けられていないプロセッサでソフトウエアを実行しようとする時に使用制限できる。番号割り当て機構は、特定のプロセッサ識別番号を持つ１つのソフトウエアに関連付けられた認可ネットワークの使用を通じて管理される。

【０００６】

上記の電子ハードウエア、コンピュータソフトウエアアプリケーションおよびデータ保護機構とは別に、音楽録音装置のようなエレクトロニクス装置によりアクセスされる他のタイプの暗号化情報の著作権侵害を防止するために行われているものは余り知られていない。

【０００７】

【発明の概要】

従来技術の特性

ソフトウエアおよび情報の不正使用を防止するための公知技術は、各種の問題を持っている。真正証明または鍵を用いるシステムは、１つの鍵でプログラムの無制限の使用が可能で、鍵のコピーを防止できない点が問題である。従って、ソフトウエアのコピーの所有者は、彼の鍵または真正証明を他者に渡すことが可能であり、この他者は真正証明または鍵を使用することにより、ソフトウエアをインストールし、作動し、または情報にアクセスすることができる。１つの鍵で１つの使用、または１回の実行のみ行う時には、コピーの問題は解決するが、この時には各使用ごとに他の鍵が必要となる。商業的には、ほとんどのプログラムは多数回の使用を必要とする。

【０００８】

ソフトウエアロックは、パーソナルコンピュータで解除することが容易である。パーソナルコンピュータの所有者はロックの解除を試みるのに、無制限の特権と時間を持つからである。ハードウエア保護方式は、ハードウエアデザイナがハードウエア装置の製作の前に保護すべきソフトウエアの性質を知ることを要求されるから、フレキシビリティを欠く。更に異なったハードウエア保護機構を用いる各種のソフトウエアが作動される時には、別個のハードウエア装置を設ける必要がある。カスタムハードウエア製作にかかるコストおよび消費者がハードウエア保護方式を使用困難と考える事実は、ハードウエア保護機構の広汎な展開を妨げる。

【０００９】

ハードウエア保護方式は、ソフトウエアを装置から装置へ移すためのフレキシビリティを制限する。ユーザーは、コンピュータ装置を買う前にソフトウエアを買うことができない。ユーザーは購入の時点で装置の識別子が何であるかを知らないからである。ハードウエアメーカーは、多くの装置に同じ装置識別子を与えることによりユーザーをごまかすことができる。最後に熟練したハッカーは、リバースエンジニアリング技法でハードウエア装置の識別子を偽造し、または装置が識別子をチェックしないように、ソフトウエアを変更する。

【００１０】

本発明の実施形態の特性

本発明は、上記の問題または他の問題を解決する。本発明は、ソフトウエアの所有者、ベンダーまたはディストリビュータ（以下、ベンダーと呼ぶ）がその知的所有権、またはそのソフトウエアにおける他の権利を保護することを可能にする方法と装置を提供する。ソフトウエアは、コンピュータプログラム、テキスト、データ、データベース、オーディオ、ビデオ、イメージ、その他デジタル的にまたは信号として表される情報のようなものを含む広い意味で定義され、上記ソフトウエアは、コンピュータまたは特殊目的の装置上でユーザーによりアクセスされ、または使用される（以下、この装置をユーザー装置と呼ぶ）。本発明は、ソフトウエアのベンダーに対してソフトウエアの使用ごとに支払う方式にすることも可能にする。

【００１１】

特に、本発明は、ユーザー装置上のソフトウエアの使用を管理し、また装置が、ソフトウエアに対する権利の正当なベンダーまたは所有者により許可されない方法で、ソフトウエアのインスタンス、つまりユーザーが使用する個々のソフトウエア、を用いることを防止する管理体制のためのシステム方法または装置を提供する。

【００１２】

特定のソフトウエアにおけるベンダーの権利は、下記に限定されない、多数の方法で侵害される。ユーザーは、購入したベンダーのソフトウエアをコピーし、これらを他者に与えることが可能であり、当該他者はソフトウエアの最初のユーザーの購入条件に基づいて許されない時にそのソフトウエアを当該他者の装置にインストールする。ある組織は、ベンダーのソフトウエアを購入し、または賃借する。そして、ソフトウエアの特定数のコピーを行い、使用することが許される場合、その特定数を上回るコピーを行う。著作権侵害ベンダーは、正当なベンダーのソフトウエアの不正コピーをつくり、販売する。著作権侵害ベンダーは、正当なベンダーのソフトウエアを改変し、例えばアプリケーションプログラムを再編集し、または歌の名前を変えるかその他の変更を行い、侵害ソフトウエアのコ

ピーを頒布し販売する。

【００１３】

本発明は、ソフトウエアにおける正当なベンダーの権利の保護を達成し、これらの権利侵害をソフトウエアのインスタンス、またはインスタンスの一部を暗号化し、ユーザーにアクセス前に解読することを要求することなく、特殊なハードウエア装置、保護装置（ドングル）、もしくは特殊なプロセッサを要求することなく、またはメーカにＩＤ番号をハードウエアに設けることをメーカに要求することなく防止する。従って、これらの方式にかかる短所および弱点は、本発明により回避される。更に本発明の方法と装置は、正当なユーザーが正当なベンダーの特定の体制に基づいて用いるソフトウエアをアクセスすることを妨げるため、非良心的な不正使用者が保護機構の利用を試みる時にも、この試みを阻止する。

【００１４】

本発明を用いることによりソフトウエアベンダーは、ユーザーに管理された方法で販売し、リースし、または頒布することを望む特定のアプリケーションプログラム、特定のブック、または歌のような特定のソフトウエアを持つ。ユーザーの装置にインストールし、またはその装置で使用することが試みられるソフトウエアの特定のコピーを、以下、ソフトウエアのインスタンスまたはソフトウエアインスタンスと呼ぶ。一般に、ソフトウエアは、以下、使用またはソフトウエアの使用と呼ぶアクセスモードの各々と共にユーザー装置にインストールされ、アクセスされ、または使用される。このようにアプリケーションプログラムである、例えばソフトウエアのインスタンスの使用は、下記に限定されることはないが、このインスタンスをインストールし、読み、コピーし、または実行することを含む。また、テキストの使用は、下記に限定されることはないが、装置上にテキストをインストールし、またテキストを装置の使用により読み、装置上でまたは装置を用いることによりこのテキストの部分をコピーすることを含む。

【００１５】

本発明の具体的な実施形態の要素およびステップ

特に、本発明は、ソフトウエアの使用を管理するためのシステムを提供する。上記のシステムは、ソフトウエアのインスタンスを作るベンダーおよびソフトウ

エアのインスタンスを受け入れるタグサーバーを有する。タグサーバーは、ソフトウエアのインスタンス当り１つのタグで複数のタグを作り、またタグはそれが関連付けられたソフトウエアのインスタンスを個々に特定する。ユーザー装置は、ソフトウエアのインスタンスを受け取り、インストールし、そして、ソフトウエアのインスタンスに個々に関連付けられたタグを受け取る。ユーザー装置は、管理プログラムを含み、これがソフトウエアのインスタンスの使用の試みを検出し、ソフトウエアのインスタンスの使用を許可する前に、ソフトウエアのインスタンスに関連付けられたタグの真正を確認する。ユーザー装置の管理プログラムは、タグの真正を確認し、タグをタグテーブルに保持または格納し、またタグが真正である時には、好ましくは格納装置にソフトウエアのインスタンスを保持し、または格納する。管理プログラムは、ソフトウエアに関連付けられたタグが真正でない時にはソフトウエアのインスタンスを拒絶する。

【００１６】

タグは、ソフトウエアのインスタンスにとって固有であることが望ましい。真正証明サーバーにより作られるタグは、ソフトウエアのインスタンスの名称、ソフトウエアのインスタンスの個々の番号および／またはソフトウエアのインスタンスの部分におけるハッシュ関数値の少なくとも１つを有する。好ましくは、ソフトウエアのインスタンスの個々の番号は、番号が疎なセットから選ばれる。他の実施形態においては、各タグは更に管理プログラムの個々の識別子を含む。更に他の実施形態においては、各タグはタグに関連付けられたソフトウエアのインスタンスの部分上で作られた少なくとも１つの指紋（電子透かし）を有する。

【００１７】

タグが真正であることを確認し決定するために、管理プログラムはタグにおけるハッシュ関数値を確認し、またはタグのデジタル署名を確認することができる。他の実施形態においては、管理プログラムは、タグにおける管理プログラムの個々の識別子がユーザー装置の管理プログラムの識別子と同じであることを確認する。指紋を用いる実施形態においては、管理プログラムはタグに関連付けられたソフトウエアインスタンスがソフトウエアのインスタンスに関連付けられたタグに含まれる少なくとも１つの指紋に対する同じ位置の指紋チェックを満足する

ことを確認する。同じ位置の指紋チェックは、ソフトウエアのインスタンス前、中および後の少なくとも１回において管理プログラムにより行う。

【００１８】

指紋を使用する実施形態において、各タグは、少なくとも１つの指紋が作られて、管理プログラムは，各タグに関連付けられたソフトウエアインスタンスの少なくとも位置の少なくとも１つのリストに定められた位置におけるソフトウエアに関連付けられた少なくとも１つの指紋に対して、同じ位置の指紋チェックを満足することを確認する。または上記に代わり一般位置指紋チェックを用いることができる（同じ位置の指紋において、位置の共通シーケンス上の２シーケンスの指紋は、第１シーケンスから第１指紋が第２シーケンスからの第１指紋に一致し、第１シーケンスからの第２指紋が第２シーケンスからの第２指紋に一致し、以下同様であれば一致する。一般位置指紋方式において、指紋の２シーケンスは、第１シーケンスにおける各指紋が第２シーケンスにおける各指紋に一致し、第２シーケンスにおける各指紋が第１シーケンスにおける各指紋に一致する時に一致する。）。タグは、ソフトウエアのインスタンスから分離しているから、本発明は、ソフトウエアを修正することを必要とせずに、ソフトウエアの保護を提供する。

【００１９】

発明の他の構成によれば、いずれかのデータファイルがソフトウエアのインスタンスによりアクセスされる時には、必ずアクセスを実施するソフトウエアのインスタンスに関連付けられた情報がデータファイルに関連付けられた位置に格納されている。ソフトウエアのインスタンスに関連付けられた情報は、ソフトウエアのインスタンスにより実行される改変の時点で、ソフトウエアのインスタンスに関連付けられたタグである。好ましくは、アクセスを実行するソフトウエアのインスタンスに関連付けられた情報は、管理プログラムのみがアクセスできる安全な位置に書き込まれる。本発明のこの構成は、共有されるソフトウエアデータを用いるソフトウエアの著作権侵害を追跡するために用いられる。

【００２０】

この場合において、ソフトウエアのインスタンスがデータファイルに関連付け

られた位置で格納される関連付けられた情報を持つデータファイル（即ち、共有されるソフトウエアデータ）をアクセスすることを試みる時には、管理プログラムは格納された関連付けられた情報が現在アクセスを試みるソフトウエアのインスタンスに関連付けられた情報であるか否かをテストする。もしこのような情報である場合には、管理プログラムはこのインスタンスが著作権侵害のコピーであると判断する。これを行うには、管理プログラムはアクセスが現在試みられるデータファイルに関連付けられた位置に格納される関連付けの情報を確認するために偽造不能なハッシュ関数を使用することができる。さらに管理プログラムは、最後の改変の時間を使用できる。本発明は、このデータファイルがこの装置におけるソフトウエアインスタンスのタグを持つソフトウエアインスタンスにより書き込まれたかを監視するものであり、その通りであれば、この装置のソフトウエアインスタンスが事実このデータを最後の改変の時点で書いたか否かを監視する。その通りでなければ、同じタグを持つ少なくとも２つのソフトウエアインスタンスが流通し、著作権の侵害が起きたのである。

【００２１】

本発明の他の実施形態は、タグの付いたソフトウエアデータベースおよび確認プログラムを持つ保護センターを有する。保護センターは、定期的にユーザー装置と呼び出し手順により通信することにより、ユーザー装置からタグを受け取る。タグは、ユーザー装置に用いられるタグ付きのソフトウエアのインスタンスに関連付けられる。確認プログラムは、タグが少なくとも１つの使用管理ポリシーが遵守されていることを確かめるためにタグ付きのソフトウエアデータベースに対してユーザー装置から受け取られた各タグを検査する。好ましくは、使用管理ポリシーは、少なくとも１つのタグが関連付けられた少なくとも１つの個別のソフトウエアのインスタンスに関連付けられる。確認プログラムは、継続メッセージをユーザー装置に戻す。継続メッセージは、ユーザー装置における各タグに関連付けられたソフトウエアのインスタンスに対して実行すべき動作（措置）を示す。ユーザー装置における管理プログラムは、真正に対する継続メッセージを確認し、真正であれば継続メッセージに示された続行すべき動作を実行する。この方法で保護センターは、タグ使用状況を管理することにより、ユーザー装置のソ

フトウエアに対するアクセスを決定することができる。

【００２２】

好ましくは、保護センターとユーザー装置との間のすべてのメッセージは安全な方法で送られ、この安全な方法は公開鍵暗号方式を含む。

【００２３】

本発明の他の構成によれば、ソフトウエアベンダー、タグサーバーおよび保護センターの少なくとも１つは、ソフトウエアベンダー、タグサーバーおよび保護センターの少なくとも他の１つと組み合わされる。

【００２４】

本発明の他の構成において、ユーザー装置の管理プログラムが保護センターと通信する時、この処理を呼び出しと呼ぶ。好ましくは、呼び出し手順の間の最大許容時間間隔は、ユーザー装置において経過する時間、ソフトウエアのインスタンスの使用の数と時間、ユーザー装置が電源オンされる度数およびユーザー装置の使用の測定の組み合わせの少なくとも１つによって決定される。ユーザー装置が最後の呼び出し手順からの最大許容時間間隔の終わりの前に保護センターを用いた呼び出し手順を行うことを怠った時には、ユーザー装置は特定時間にわたり機能を停止され、またはソフトウエアのインスタンスの使用は特定時間帯にわたり否定される。好ましくは、ソフトウエアのインスタンスがユーザー装置において初めて用いられる（即ち、アクセス、インストール、またはその他の形で検出される）時には、呼び出しが行われる。または、呼び出しは保護センターからのリクエストにより生じる。

【００２５】

本発明の１つの構成によれば、呼び出し中、管理プログラムは、継続メッセージ中のタグテーブルのハッシュ関数値がユーザー装置からの呼び出しメッセージで送られるタグテーブルのハッシュ関数値に等しいことを確認することにより継続メッセージの真正をテストする。継続メッセージ中のデジタル署名を確認することにも用いられる。

【００２６】

呼び出しメッセージに続いて、保護センターへの継続メッセージをユーザー装

置が受け取らない時には、ユーザー装置は前の呼び出しメッセージに対するキャンセル指令を用いた呼び出しメッセージを再度送ることができる。この構成によりユーザー装置は、呼び出しを再び試みることができる。

【００２７】

保護センターにおいて、使用管理ポリシーが呼び出し手順中に保護センターと通信する全ユーザー装置に関連付けられるか、使用管理ポリシーが呼び出し手順中に保護センターと通信するユーザー装置の個々のユーザーに関連付けられるか、または使用管理ポリシーが呼び出し手順中に保護センターと通信するユーザー装置の使用管理履歴に関連付けられる。

【００２８】

本発明の他の構成によれば、保護センターは各ユーザー装置上のソフトウエアの各インスタンスに関連付けられた各タグに対するタグ付きのソフトウエアデータベースのタグデータ構造体を保持する。各タグデータ構造体は、ソフトウエアのインスタンスタグ、ソフトウエアのインスタンスに関連付けられた使用管理ポリシーおよび呼び出し記録についての参照の収集物（集合体）を有する。呼び出し記録の収集物中の各呼び出し記録は、１つの呼び出し手順に関する情報を表わす。呼び出し手順に関連付けられた継続メッセージは、少なくとも１つの呼び出し時間、呼び出し手順中の保護センターに移行するタグテーブルのヘッダ、前の呼び出し手順のタイムスタンプを示す最後の呼び出し時間、呼び出し手順中の保護センターに移されるタグテーブルのハッシュ関数値およびユーザー装置が続行する動作を有する。前の呼び出し記録を保存する理由は、１つの装置のみがタグテーブルの特定のヘッダを持つことを保護センターが確認できるようにすることにある。これが行われなければ、各種の物理的装置が使用管理ポリシーに違反して同じソフトウエアインスタンスを共有することが可能となる。

【００２９】

保護センターまたはこれと組み合わされた装置においては、保護センターは確認プログラムを有する。この構成によれば、保護センターはユーザー装置からユーザー装置の管理プログラムのための個々の識別子を受け取るための呼び出し手順を介してユーザー装置と定期的に通信する。確認プログラムは、その識別子を

持つのは多くても１つの管理プログラムであることを確かめるために個々の識別子を調べる。そして、確認プログラムは継続メッセージをユーザー装置に戻す。継続メッセージは、ユーザー装置上の各タグに関連付けられたソフトウエアのインスタンスの使用の試みを続行するための動作を示す。ユーザー装置の管理プログラムは、真正に対する継続メッセージを確認し、真正であれば継続メッセージにおける動作を実行する。

【００３０】

保護センターのこの実施形態によれば、管理プログラムの識別子は、管理プログラムが最初に作動される時に、ほとんど重複しない番号に基づいて作られる。好ましくは、上記番号は、管理プログラムが装置上で最初に作動される時に生じる極めて正確なクロック値である。上記に代えて、上記番号は保護センターにより与えられてもよい。上記一方または組み合わせにより、メモリ位置の値によって与えられてもよい。

【００３１】

本発明の他のシステムによれば、このシステムは、ユーザー装置に用いられるソフトウエアのタグのないインスタンスをも含む。このシステムにおいて管理プログラムは、タグのないソフトウエアのインスタンスの使用を検出し、タグのないソフトウエアのインスタンスにおいて指紋処理を行い、ユーザー装置の指紋処理からの指紋を格納する。ユーザー装置の管理プログラムは、更に装置に用いられるソフトウエアのタグ付きインスタンスにおいて指紋処理を行い、ユーザー装置の指紋テーブルの指紋処理から生じる指紋を格納する。管理プログラムは、指紋が作られる位置を格納する。指紋は、ソフトウエアのインスタンスの内容に基づいてもよい。また、上記に代えて、指紋はソフトウエアのインスタンスの挙動のシーケンスに基づいてもよい。

【００３２】

このシステムにおける保護センターの実施形態によれば、保護センターは、指紋データ構造体および確認プログラムを有する。保護センターは、ユーザー装置で用いられるソフトウエアのインスタンスに対してユーザー装置からすべての指紋を受け取るように、呼び出し手順を介してユーザー装置と定期的に通信する。

確認プログラムは、ユーザー装置から受け取ったすべての指紋を指紋データ構造体と比較することにより、ユーザー装置に用いられるソフトウエアのインスタンスがソフトウエアの侵害インスタンスであるか否かを判断する。確認プログラムが保護センターの指紋データ構造体とユーザー装置から受け取られた指紋との間で指定数以上の一致を検出した時には、確認プログラムは実行すべき報復措置を特定し、確認プログラムは継続メッセージをユーザー装置に戻す。継続メッセージは、ユーザー装置で実行される報復措置を示す。

【００３３】

ソフトウエアベンダーは、ソフトウエアの侵害インスタンスのコピーを保護センターに送り、保護センターは、ソフトウエアの侵害インスタンスのコピー上の指紋を算定し、保護センターの指紋データ構造体の中に指紋を格納する。

【００３４】

このシステムの１つの構成によれば、指紋一致処理は、一般的な位置指紋チェックである。処理を速めるために指紋一致は、反転保護センター指紋テーブルを使用する。

【００３５】

報復措置は、ユーザー装置が指定時間にわたり機能を停止されるか、または保護センターの指紋データ構造体の指紋に一致した指紋に関連付けられたソフトウエアのインスタンスが指定時間にわたり機能停止されるかを指定できる。報復措置は、ユーザー装置の挙動履歴の組み合わせ、ユーザー装置における特定ユーザーの挙動履歴およびユーザー装置におけるソフトウエア供給の集合の少なくとも１つによって特定される。

【００３６】

本発明の他の実施形態は、ユーザー装置の読み取り可能媒体、例えば装置読み取り可能媒体で符号化されたタグデーブルデータ構造体を提供する。タグテーブルデータ構造体は、ソフトウエアの１つのインスタンスに個々に関連付けられた少なくとも１つのタグを有し、タグテーブルのタグに関連付けられた少なくとも１つの領域およびソフトウエアのインスタンスに関連付けられたタグに関連付けられた使用状況を示す少なくとも１つの領域を有する。少なくとも１つの領域は

、タグに関連付けられたソフトウエアの１つのインスタンスに対する使用統計を示す。タグテーブルは、タグテーブルを個々に識別するタグテーブルヘッダを有する。タグテーブルヘッダは、ユーザー装置の使用統計に関する情報を有し、同様に継続メッセージをも有することができる。タグテーブルは、ユーザー装置で用いられるべきソフトウエアのインスタンスの能力に関する情報を格納するために用いられる。

【００３７】

本発明の装置と方法は、それぞれ少なくとも１つの名称とソフトウエアの内容を持つソフトウエアのインスタンスを形成するソフトウエア形成機構からなるソフトウエアベンダーを有する。ソフトウエアの各インスタンスは、ソフトウエアのインスタンスごとのタグに関連してのみ使用できる。好ましくは、タグはタグが関連付けられたソフトウエアのインスタンスに関する個々に偽造不能な情報の収集物であり、ソフトウエアの１つの名称、ソフトウエアのインスタンスの番号、ソフトウエアの内容の一部におけるハッシュ関数値、ソフトウエアのインスタンスが使用されるべきユーザー装置に関連付けられた管理プログラムの識別子、またはタグが関連付けられたソフトウエアのインスタンスの部分の指紋リストの少なくとも１つを有する。

【００３８】

本発明の他の実施形態によれば、ソフトウエアベンダーは、ベンダーの権利を侵害するソフトウエアを検出し、侵害ソフトウエアのコピーを保護センターに送ることにより、ユーザー装置で侵害ソフトウエアのインスタンスの試みられた使用を検出するように使用管理を実施できる侵害ソフトウエア検出機構を有する。

【００３９】

この実施形態の他の構成によれば保護センターは、侵害ソフトウエアのインスタンスに関連付けられたタグを無効化し、保護センターにより侵害ソフトウエアのインスタンスを使用したことを検出されたユーザー装置に報復措置を送ることができる。

【００４０】

本発明の他の実施形態は、ソフトウエアのインスタンスを受け入れ、ソフトウ

エアインスタンスに個々に関連付けられたタグを受け入れ、そしてソフトウエアのインスタンスを使用することのリクエストを受ける入力ボードを含むユーザー装置である。ユーザー装置に含まれるプロセッサは、管理プログラムを実行する。管理プログラムは、ソフトウエアのインスタンスを使用するためのリクエストを検出し、ユーザー装置によるソフトウエアのインスタンスの使用許可の前に、ソフトウエアのインスタンスに関連付けられたタグが真正であることを確認する。管理プログラムは、タグが真正であることを確認し、タグテーブルにおけるタグを格納し、タグが真正であればソフトウエアのインスタンスを保持し、ソフトウエアに関連付けられたタグが真正でなければソフトウエアのインスタンスを拒絶する。

【００４１】

ユーザー装置の１つの構成によれば、管理プログラムは、ソフトウエアのインスタンスにおけるハッシュ関数値を算定し、算定値をタグのハッシュ関数値と比較することによりタグが真正であるか否か、またソフトウエアのインスタンスに正しく関連付けられているか否かを判断する。好ましくは、タグはデジタル的にサインされ、管理プログラムはタグのデジタル署名を確認することによりタグが真正であることを確認する。

【００４２】

ユーザー装置の中で、タグテーブルはユーザー装置に格納されるデータ構造体であり、ソフトウエアのインスタンスに個々に関連付けられた少なくとも１つのタグを有し、タグテーブルの中のタグに関連付けられた少なくとも１つの領域を有し、この少なくとも１つの領域はタグに関連付けられたソフトウエアのインスタンスに対する使用状況を示す。管理プログラムは、呼び出し手順が呼び出し方式により定められたようにリクエストされることを定期的に決定し、そしてタグテーブルに格納されているタグの使用状況を更改するための呼び出し手順を実行する。

【００４３】

管理プログラムは、ダグ付きのソフトウエアにより用いられる各データファイルが正当なソウトウエアのインスタンスにより形成されていることを確認する。

【００４４】

呼び出し手順の実行中、管理プログラムは、ユーザー装置に結合された相互接続機構を介してユーザー装置からのタグテーブルを安全に送り、ユーザー装置に戻される継続メッセージの受け入れを待つ。上記継続メッセージはタグテーブルの各タグに対して実行すべき動作を示す。また、呼び出し手順の実行中にも、管理プログラムは、ユーザー装置に結合された相互接続機構を介してユーザー装置からのタグテーブルヘッダを安全に送り、タグテーブルの各タグに対して実行されるべき動作を示すユーザー装置に戻される継続メッセージの受け入れを待つ。

【００４５】

本発明の他の実施形態は、タグなしのソフトウエアの使用を管理することを可能にする。この実施形態によるユーザー装置は、ユーザー装置に用いられるタグのないソフトウエアのインスタンスを有する。管理プログラムは、ソフトウエアのタグなしのインスタンスを検出し、指紋処理を実施し、ユーザー装置の指紋テーブルにおける指紋処理から得られた指紋を格納する。管理プログラムは、呼び出し手順が呼び出し方式によって定められるようにリクエストされることを決定し、管理プログラムは呼び出し手順を実行することによりユーザー装置に格納されるタグのないソフトウエアのインスタンスの使用状況を更新する。このようにタグのないソフトウエアの管理は、タグ付きのソフトウエアの存在、または管理とは無関係に行うことができる。

【００４６】

呼び出し手順を行う時に、管理プログラムは、ユーザー装置に結合された相互接続機構を介してユーザー装置から指紋テーブルの部分を送り、ユーザー装置に格納された各タグのないソフトウエアのインスタンスに対して実行すべき動作を示すユーザー装置に戻された継続メッセージの受け取りを待つ。

【００４７】

本発明の他の実施形態によれば、保護センターは、タグ付きのソフトウエアデータベースおよび保護センターのプロセッサで実行する確認プログラムを含むものが設けられている。保護センターは、相互接続機構を介してソフトウエアのインスタンスに対するタグを受け取るための呼び出し手順を定期的に実行する。確

認プログラムは、タグが少なくとも１つの使用管理ポリシーに従うものであることを確かめるために保護センターに保持されるタグ付きソフトウエアデータベースを用いて受け取られた各タグを検査する。確認プログラムは、相互接続機構を介して呼び出し手順中に保護センターにより受け入れられる各タグに関連付けられたソフトウエアのインスタンスの試みられた使用を続行するように動作を示す継続メッセージを送る。

【００４８】

この実施形態のある構成によれば、使用管理ポリシーは、少なくとも１つのタグが関連付けられたソフトウエアの各インスタンスに関連付けられる。また、使用管理ポリシーは、保護センターがタグを受け取るために通信するユーザー装置に関連付けられる。使用管理ポリシーは、保護センターがタグを受け取るために通信するユーザー装置の個々のユーザーに関連付けられる。

【００４９】

保護センターは、各ユーザー装置のソフトウエアのインスタンスに関連付けられた各タグに対するタグ付きソフトウエアデータベースのタグデータ構造体を保持し、タグサーバーからソフトウエアのインスタンスに関連付けられた新たに作られたタグを受け取り、更にユーザー装置から送られたタグテーブルのユーザー装置で用いられるソフトウエアのインスタンスに関連付けられたタグを受け取る。各タグデータ構造体は、ソフトウエアのインスタンスのタグ、ソフトウエアのインスタンスの名称、ソフトウエアのインスタンスの番号、ソフトウエアのインスタンスのハッシュ関数値、ソフトウエアのインスタンスに関連付けられた使用管理ポリシーおよび上記ソフトウエアのインスタンスに関連付けられたタグに関連付けられた呼び出し記録についての参照の収集物の少なくとも１つを有する。

【００５０】

呼び出し記録の収集物における各呼び出し記録は、１つの呼び出し手順に関する情報を表し、呼び出し時間、呼び出し手順中に保護センターに送られたタグテーブルのヘッダ、前の呼び出し手順のタイムスタンプを示す最後の呼び出し時間、呼び出し手順中の保護センターに送られたタグテーブルのハッシュ関数値および呼び出し手順に関連付けられた継続メッセージに含まれるユーザー装置を続行

するための動作の少なくとも１つを有する。

【００５１】

この発明による保護センターの他のタイプは、指紋データ構造体および確認プログラムを実行するプロセッサを有する。確認プログラムは、ユーザー装置で用いられるソフトウエアのインスタンスに対する指紋を相互接続機構を介して受け取るようにユーザー装置に対して呼び出し手順を定期的に実行する。確認プログラムは、指紋データ構造体に対して受け取られた各指紋を検査することにより、ユーザー装置に用いられたタグのないソフトウエアのインスタンスがソフトウエアの侵害インスタンスであるか否かを調べ、侵害インスタンスであれば、確認プログラムはユーザー装置に対して実行されるべき報復措置を生成する。

【００５２】

ある実施形態においては、すべてのベンダーソフトウエアは指紋が作られ、１つのベンダーソフトウエアによる他のベンダーソフトウエアに対する侵害が一般位置指紋チェックに基づいて検出される。確認プログラムが指紋データ構造体と受け取った指紋の中における指紋との間で充分な数の一致を検出する時には、確認プログラムは実行されるべき報復措置を特定し、確認プログラムは継続メッセージを送る。上記継続メッセージは継続メッセージの受信機に対して実行される報復措置を示す。充分な数の一致は１つ以上であるか、または各一致の重みが一致する指紋によって変化する時には、一致の加重合計値として算定される。

【００５３】

この実施形態の他の構成によれば、報復措置は受信機の機能停止、または指紋データ構造体の中の指紋に一致した指紋に関連付けられたソフトウエアのインスタンスが機能停止されるべきことが特定される。

【００５４】

他の方法では、保護センターで確認プログラムが相互接続機構を介してソフトウエアの侵害インスタンスのコピーを受け取り、タグのないソフトウエアインスタンスのコピーを受け取り、タグのない侵害ソフトウエアインスタンスのコピー上の指紋を算定し、指紋を指紋データ構造体に入れて格納する。

【００５５】

本発明の実施形態は、特定のベンダーソフトウエアのコピーを受け入れ、複数のタグをソフトウエアインスタンス当り１つの割合で作り、上記各タグが関連付けられたソフトウエアのインスタンスを個々に識別するものであるタグサーバーを有する。好ましくは、各タグは、タグに関連付けられたソフトウエアの名称、タグに関連付けられたソフトウエアのインスタンスの番号、およびタグに関連付けられたソフトウエアのインスタンスの部分において算定されたハッシュ関数値の少なくとも１つを有する。タグをデジタル的にサインし、タグを例えばユーザー装置、保護センター、またはソフトウエアベンダーのような受信機に安全に送るためにデジタル署名機構を用いることができる。

【００５６】

本発明にかかる方法は、ソフトウエアの使用を管理するための方法を有する。この方法は、ソフトウエアのインスタンスを作り、ソフトウエアのインスタンスに個々に関連付けられるタグを作るステップを有する。次にソフトウエアのインスタンスを配布し、タグをユーザー装置に安全に配布し、そして、ユーザー装置のタグおよび関連付けられたタグを受け取る。次にユーザー装置のソフトウエアのインスタンスを使用するための試みを検出し、そのソフトウエアのインスタンスを使用するための試みが、使用されるべきソフトウエアのインスタンスに関連付けられたタグのステータスを判断することによって許容されるか否かを判断する。

【００５７】

上記の方法において，タグ製作は、ソフトウエアのインスタンスに対する番号を割り当て、ソフトウエアのインスタンスの内容の部分での第１ハッシュ関数値を算定するステップを有する。次に、ソフトウエアのインスタンスに対する第２ハッシュ関数値を算定することを有し、上記第２ハッシュ関数値はソフトウエアの名称、ソフトウエアのインスタンスの番号および第１ハッシュ関数値を組み合わせる。次に、ソフトウエアのインスタンスに個々に関連付けられたタグを算定するステップを有し、上記タグはソフトウエアの名称、ソフトウエアのインスタンスの番号および第２ハッシュ関数値を有する。

【００５８】

タグを作るステップは、署名を作るための第２のハッシュ関数値にデジタル署名機能を適用し、署名をタグに含めることによりデジタル的にサインされたタグを作る。

【００５９】

タグをユーザー装置に配布するステップは、公開鍵暗号技術を用いてソフトウエアベンダーおよびユーザー装置に安全にタグを配布するステップを有する。

【００６０】

ソフトウエアのインスタンスを受け取るステップは、ユーザー装置においてソフトウエアのインスタンスを入手するステップを有する。ユーザー装置のタグを受け取るステップは、ユーザー装置におけるソフトウエアのインスタンスに関連付けられたタグを安全に受け取り、ソフトウエアのインスタンスに関連付けられたタグがサインされたか否かを判断し、サインされている時には、タグのハッシュ関数値の署名を確認し、ハッシュ関数値上の署名が確認されるとユーザー装置上にソフトウエアをインストールし、ソフトウエアインスタンスに関連付けられたタグがサインされていない時には、ユーザー装置上にソフトウエアのインスタンスをインストールするステップを有する。ユーザー装置でソフトウエアインスタンスを使用する試みを検出するステップは、ソフトウエアのインスタンスの使用に対するユーザーのリクエストを阻止するためにユーザー装置に管理プログラムを作動させるステップを有する。ソフトウエアインスタンスを用いる試みが許されるか否かを判断するステップは、呼び出し手順が呼び出し方式に基づいて必要とされるか否かが判断され、必要とされる場合には、呼び出し手順を行うことにより真正であることを確認し、ソフトウエアインスタンスに関連付けられたタグの使用管理ポリシーを決定するステップを有する。また、呼び出し手順の結果に基づいてユーザー装置におけるタグ情報を更新するステップを有し、タグに関連付けられたソフトウエアのインスタンスの使用が許されるか否かを判断するためにタグに関連付けられたステータス情報を検査するステップを有する。

【００６１】

呼び出し手順を実行するステップは、ユーザー装置からのソフトウエアのインスタンスに関連付けられたタグを格納するタグテーブルを送るステップと、タグ

テーブルにおける各タグに対して実行されるべき動作を示すユーザー装置に戻される継続メッセージの受け取りを待つステップとを有する。ユーザー装置は、継続メッセージを待つ間、実行のための端末リクエストの処理を継続する。

【００６２】

方法の実施形態は、継続メッセージが特定の装置に向かって送られるステップ、およびイベント履歴がこの装置のイベント履歴に対応することを確認するステップを有する。

【００６３】

方法の実施形態において、呼び出し手順を実行するステップは、ソフトウエアのインスタンスに関連付けられたタグを含むタグテーブルを受け取るステップと、タグテーブルのタグが少なくとも１つの使用管理ポリシーに従っていることを確かめるためのタグ付きのソフトウエアデータベースに対してタグテーブルに受け取られた各タグを検査するステップを有する。また、各タグに関連付けられたソフトウエアのインスタンスの使用の試みを検出した時にユーザー装置で続行するための動作を示す継続メッセージを送るステップも含まれる。

【００６４】

方法の実施形態において、継続メッセージには、継続メッセージが送られる相手の管理プログラムの管理プログラム識別子、継続メッセージが準備された時点および装置からの呼び出しに伴うタグテーブルヘッダの暗号化を含むことができる。

【００６５】

ソフトウエアの使用を管理するための方法は、本発明の一部として提供され、ユーザー装置上のタグのないソフトウエアのインスタンスの使用を検出し、ユーザー装置上のタグなしのソフトウエアインスタンスに関連付けられた指紋を作り、格納するステップを有する。続いて、ユーザー装置におけるタグのないソフトウエアのインスタンスを使用することの試みを検出し、ソフトウエアのインスタンスを使用することの試みがタグのないソフトウエアのインスタンスに関連付けられた指紋を侵害指紋の指紋データ構造体と比較することにより有効であるか否かを判断し、指紋が一致する時には、タグのないソフトウエアのインスタンスの

使用を機能停止する。

【００６６】

上記の方法は、ユーザー装置上のタグ付きのソフトウエアのインスタンスの使用を検出するステップ、およびユーザー装置のタグ付きのソフトウエアのインスタンスに関連付けられた指紋を作り、格納するステップを有する。ユーザー装置のタグ付きのソフトウエアのインスタンスを使用する試みを検出するステップは、ソフトウエアのインスタンスを使用することの試みが、タグ付きのソフトウエアのインスタンスに関連付けられた指紋を侵害指紋の指紋データ構造体と比較することにより有効であるか否かを判断し、指紋が一致する時には、タグ付きのソフトウエアのインスタンスの使用の機能を停止するステップである。

【００６７】

上記の方法は、ソフトウエアベンダーにより侵害ソフトウエアのインスタンスを検出し、侵害ソフトウエアのインスタンスのコピーを保護センターに提出するステップにより補足される。保護センターでソフトウエアの侵害インスタンス上の指紋を作り、指紋を指紋データ構造体に格納するステップも含まれる。この補足的な方法は、タグ付きのソフトウエアの存在に関係がなく、他の実施形態でもあり得る。

【００６８】

本発明の他の実施形態は、ソフトウエアのインスタンスを入手し、ソフトウエアのインスタンスに名称を割り当て、そしてソフトウエアのインスタンスに番号を割り当てるステップを持つソフトウエアのインスタンスを個々に識別するための方法を有する。上記番号は、同じソフトウエアの他のインスタンスに割り当てられた番号とは異なることがある。この方法は、ソフトウエアのインスタンスの部分におけるハッシュ関数値を算定し、インスタンスソフトウエアの名称のシーケンスにおける第２ハッシュ関数値、インスタンスソフトウエアの番号、およびソフトウエアインスタンスごとの署名のないハッシュ関数値を作るための第１ハッシュ関数値を算定するステップをも有する。続いて、ソフトウエアのインスタンスに対する署名されたハッシュ関数値を作るための鍵を用いて署名されないハッシュ関数値を署名し、ソフトウエアのインスタンスを個々に識別するソフトウ

エアのインスタンスに関連付けられたタグを作る。上記タグはソフトウエアのインスタンスの署名されたハッシュ関数値、ソフトウエアのインスタンスの名称、ソフトウエアのインスタンスの番号およびインスタンスソフトウエアの署名をされないハッシュ関数値を有する。

【００６９】

この実施形態によれば、ソフトウエアのインスタンスを入手し、ソフトウエアベンダーにより実行されるソフトウエアに名称を割り当て、ソフトウエアのインスタンスに番号を割り当て、第１および第２ハッシュ関数値を算定し、第２ハッシュ関数値に署名し、そしてタグサーバーによって実行されるタグを作るステップがある。

【００７０】

本発明は、プロセッサにおいて読み取られ実行される時にソフトウエアのインスタンスを使用するためのリクエストを検出し、ソフトウエアのインスタンスに対応するタグがソフトウエアのインスタンスが使用されることが許容される関連付けられたステータスを持つか否か判断し、タグの真正であることを確認し、タグに対応するソフトウエアのインスタンスが使用管理方式に従って用いられることを確実にするために呼び出し手順を定期的に実行する指示により、符号化されたコンピュータで読み取り可能媒体に関する実施形態を有する。

【００７１】

本発明は、通信媒体を通じ搬送波を介して伝送される伝播信号についての実施形態も有する。このような信号は、ソフトウエアのインスタンスに個々に関連付けられた少なくとも１つのタグ、タグテーブルのタグに関連付けられた少なくとも１つの領域、およびタグに関連付けられたソフトウエアの１つのインスタンスに対する使用管理ステータスを示す少なくとも１つの領域を有する符号化されたタグテーブルデータ構造体を搬送する。

【００７２】

また、このような信号は符号化された継続メッセージを搬送する。上記継続メッセージは動作に関連付けられたソフトウエアのインスタンスを使用する試みが受信機により検出される時に伝播信号の受信機において実行されるべき動作の指

示を有する。

【００７３】

他の方法は、ソフトウエアプログラムが改変されていないことを確かめるためのものである。この方法の実施形態は、ソフトウエアプログラムの内容に関する偽造不能なハッシュ関数値を算定し、偽造不能なハッシュ関数値の結果を前回保持されたハッシュ関数値の結果と比較することにより、結果が同じであるか否か判断し、ソフトウエアプログラムが改変されていれば指示するステップを有する。この方法の１つのバージョンにおいて、オペレーティングシステムが偽造不能なハッシュ関数値を算定し、ソフトウエアプログラムは管理プログラムである。

【００７４】

また、本発明によって、データの内容に関して偽造不能なハッシュ関数値を算定し、この値を前に算定されたハッシュ関数値と比較することにより、当該データが改変されていないことを確かめる方法が提供される。好ましくは、管理プログラムは、偽造不能なハッシュ関数値およびこの方法で管理プログラムにより用いられたデータを算定する。

【００７５】

上記の実施形態について詳細な記述を行う前に、一般的な高レベルの作用についての要旨を以下に記載して、発明の実施形態の複雑な部分についての理解の助けとする。

【００７６】

上記の実施形態に記載されているように、ベンダーの特定のソフトウエアの各インスタンスには、個々の偽造不能なタグが添付される。しかし、同じ特定のソフトウエアのすべてのソフトウエアインスタンスは同一で、暗号化されておらず、それぞれ特定のソフトウエアのコピーからなり、大抵ソフトウエアの名称を有する。例えば、特定のアプリケーションプログラムソフトウエアのインスタンス“スプレッド（展開）”は、スプレッドシートアプリケーションのためのプログラムコードおよび名称スプレッドを有する。本発明では、特他のハードウエア装置が必要でないから、任意の種類のソフトウエアのインスタンスが共通の装置または異なった装置に使用できる。

【００７７】

ソフトウエアベンダーは、特定のソフトウエアのインスタンス（コピー）を作り、このソフトウエアの１つのインスタンスを、このソフトウエアのインスタンスについてのタグ番号に対するリクエストと共に、タグサーバーに送る。タグサーバーは、異なったタグのリクエスト番号を作る。各タグは、ベンダーによってソフトウエアの１つのインスタンスで関連付けられ、それが関連付けられたソフトウエアのインスタンスを個々に識別するのに役立つ。ユーザー装置は、ベンダーのソフトウエアのインスタンスを受け取り、使用することを試み、ソフトウエアのインスタンスに個々に関連付けられたタグを確実に受け取る。

【００７８】

ユーザー装置は、装置上で作動する管理プログラムを包含し、このプログラムは関連付けられたタグが真正であることを確認し、タグテーブルにタグを格納し、格納装置にソフトウエアのインスタンスを格納し、タグが真正である時にのみソフトウエアインスタンスの使用を許可する。管理プログラムは、インスタンスに関連付けられたタグが真正でない時にのみソフトウエアインスタンスを拒絶する。タグテーブルにおけるすべてのタグは、管理プログラムによりそれに関連付けする“ユーザブル（使用可能）”、“リムーブド（除去された）”または“ペイパーユーズ（使用ごとの支払）”のようなステータスを持つ。管理プログラムは、ソフトウエアのインスタンスを使用するための装置へのコマンドを検出し、ソフトウエアのインスタンスに関連付けられたタグに関連付けられたステータスを確認し、そのインスタンスの使用を許可する。

【００７９】

データまたはデータを有するオブジェクトを安全に送りまたは受け取ることは、データまたはオブジェクトに含まれるデータが、承認された送信者または受信者以外の何者かにより改変されまたは開示されることを許さない方法で、送信されまたは受信されていることを意味する。例えば、タグは、ベンダーからユーザー装置へＴＥＴＳ　ＩＳＰＥＣ、ネットスケープ　ＳＳＬ、または通信を確保する他のプロトコルの使用によるネットワークによって安全に送られる。また、タグはタンパー（いたずら）防止シールされた封印に入れられたディスケットを用

いてベンダーからユーザーに渡される。安全な通信は、盗用者による情報の漏洩を防止するために用いられるもので、本発明の保護機構の一部ではない。当事者間の安全な通信のための標準プロトコルがこの目的に用いられる。

【００８０】

上記の実施形態に記載されたように、ベンダーソフトウエアのインスタンスに対するタグサーバーにより作られるタグは、そのソフトウエアの名称、ソフトウエアのインスタンスに対する個々の識別番号（以下、インスタンス番号と呼ぶ）、ソフトウエアのインスタンス部分のハッシュ関数値およびすべての前のデータを組み合わせるハッシュ関数値を有する。本発明に用いられているインスタンス番号は、整数または任意のシンボルの連続であることが可能であり、上記の連続は個々の識別子としての役割を果す。また、タグサーバーは、最後に述べたハッシュ関数値をデジタル的に署名し、タグの中で署名してもよい。

【００８１】

以下、署名を有するタグを署名されたタグと呼び、署名を含まないタグを署名されないタグと呼ぶ。ソフトウエアＳＷのインスタンスＩＮＳＴ＿ＳＷに対する署名されないタグを作る時には、タグサーバーはソフトウエアＳＷに関連付けられた、疎で秘密の番号セット（以下、疎セットと呼ぶ）からインスタンスの識別番号を選択する。秘密スパースセットの番号は、例えば物理的処理により生成できる。

【００８２】

ソフトウエアのインスタンスＩＮＳＴに関連付けられたタグが真正であるか否かを判断するために、ＩＮＳＴが設置されまたは使用される装置の管理プログラムは、インスタンス番号ＩＮＳＴのＮＵＭ＿ＩＮＳＴおよび名称ＳＷのＮＡＭＥ＿ＳＷをタグから抽出する。管理プログラムは、ソフトウエアＩＮＳＴの内容の特定部分に関するハッシュ関数値を算定する。管理プログラムは、次にインスタンス番号ＮＵＭ＿ＩＮＳＴ、名称ＮＡＭＥ＿ＳＷおよび前に算定されたハッシュ関数値を組み合わせるハッシュ関数値を算定する。管理プログラムは、算定されたハッシュ関数番号をタグの中で発見されたハッシュ関数値と比較する。管理プログラムは、署名されたタグを構成するデジタル署名を確認する必要がある。署

名のないタグが真正であることは、タグをタグサーバーまたはタグの真正を証明する次述の保護センターに安全に送ることによって、ソフトウエアの関連付けられたインスタンスの最初またはその後の使用を許可する前に管理プログラムによりチェックされる。

【００８３】

上述のように上記システムは、タグ付鍵のソフトウエアデータベースおよび確認プログラムを有する保護センターを有する。保護センターは、ユーザー装置にインストールされた各ソフトウエアのインスタンスに対しユーザー装置からすべてのタグを受け取るために、呼び出し手順を介してユーザー装置と定期的に通信する。確認プログラムは、タグが少なくとも１つの使用管理ポリシーに従うことを確保するために、タグ付きのソフトウエアデータベースを用いてユーザー装置から受け取った各タグを検査する。確認プログラムは、ユーザー装置上の各タグに関連付けられたソフトウエアのインスタンスへ試みられたアクセスを続行するための動作を示すユーザー装置へ継続メッセージを戻す。

【００８４】

使用管理ポリシーは、少なくとも１つのタグが関連付けられているソフトウエアの個別のインスタンスに関連付けられるか、保護センターが通信する相手の全ユーザー装置に関連付けられるか、または保護センターが通信する相手のユーザー装置の個別のユーザーに関連付けられる。

【００８５】

保護センターは、各ユーザー装置の各ソフトウエアのインスタンスに対し各タグに対するタグ付きのソフトウエアデータベースにおけるタグデータ構造体を保持する。各タグデータ構造体は、ソフトウエアのインスタンスのタグ、ソフトウエアのインスタンスの名称、ソフトウエアのインスタンスの固有の番号、ソフトウエアのインスタンスのハッシュ関数値、ソフトウエアのインスタンスに関連付けられたポリシーおよびソフトウエアのインスタンスに関連付けられた一連の呼び出し記録を有する。一連の呼び出し記録の中の各呼び出し記録は、１つの呼び出し手順に関する情報を表し、呼び出し時間、呼び出し手順中に保護センターに搬送されたタグテーブルのヘッダ、前の呼び出し手順のタイムスタンプを示す最

後の呼び出し時間、呼び出し手順中の保護センターに搬送されたタグテーブルのハッシュ関数値および呼び出し手順に関連付けられた継続メッセージに含まれるユーザー装置が続行するための動作を有する。これらの機構を用いることにより保護センターは、インスタンスの使用ごとに支払うような動作に対しソフトウエアのインスタンスの使用統計を追跡できる。

【００８６】

本発明の他の構成によれば、タグのないソフトウエアのインスタンスは、ユーザー装置にインストールすることができる。保護プログラムは、タグのないソフトウエアのインスタンスを検出し、タグのないソフトウエアのインスタンスに指紋処理を実行し、ユーザー装置の指紋テーブルにおける指紋処理から得られた指紋を格納する。保護センターは、この構成によれば指紋データベースを有する。保護センターは、ユーザー装置にインストールされたタグのないソフトウエアのインスタンスに対するユーザー装置からのすべての指紋を受け取るために呼び出し手順を介してユーザー装置と定期的に通信を行う。確認プログラムは、指紋データベースによりユーザー装置から受け取った各指紋を検査することにより、タグのないソフトウエアのインスタンスがソフトウエアの侵害インスタンスではないかを判断する。この方法で本発明は、不正コピーである改変されたソフトウエアの使用を検出できる。

【００８７】

確認プログラムがユーザー装置から受け取ったすべての指紋中の１つの指紋と指紋データベース中の指紋との一致を検出した時に、確認プログラムは、報復措置の実行を特定し、確認プログラムは継続メッセージをユーザー装置に戻す。この場合、継続メッセージはユーザー装置に実行されるべき報復措置を示す。従って、ユーザー装置は、例えばタグのない侵害ソフトウエアの使用が見つけられた時には機能停止される。

【００８８】

また、報復措置は、指紋データベース中の１つの指紋に一致した指紋に関連付けられたタグのないソフトウエアのインスタンスが機能停止されるようにしてもよい。

【００８９】

指紋を保護センターで入手するために、ソフトウエアベンダーは、タグのないソフトウエアの侵害インスタンスのコピーを保護センターに送り、保護センターはタグのないソフトウエアの侵害インスタンスのコピーで指紋を算定し、上記指紋を指紋データベースに格納する。

【００９０】

本発明の他の実施形態は、装置読み取り可能媒体上で符号化されたタグテーブルデータ構造体を提供する。タグテーブルデータ構造体は、ソフトウエアの１つのインスタンスで固有に識別される少なくとも１つのタグと、タグテーブル中のタグに関連付けられた少なくとも１つの領域を有する。上記の領域は、タグで識別されたソフトウエアの１つのインスタンスに対する使用管理ステータスを示し、タグで識別されたソフトウエアの１つのインスタンスに対する使用統計も示す。タグテーブルデータ構造体は、タグテーブルを固有に識別し、タグテーブルを固有に１つのユーザー装置に関連付けられたタグテーブルヘッダをも有する。タグテーブルヘッダは、ユーザー装置の使用統計に関する情報と、継続メッセージとを有する。継続メッセージは、タグに関連付けられたソフトウエアのインスタンスに対する報復措置および使用管理ステータスを示す。

【００９１】

ソフトウエアベンダーは、本発明の１つの構成として、名称とソフトウエアの内容を持つソフトウエアのインスタンスを作るソフトウエア開発機構を有する。各ソフトウエアのインスタンスは、ソフトウエアのインスタンスに固有なタグと結合してのみ実行可能となる。上記のタグは、それが関連付けられ、ソフトウエアの名称、ソフトウエアのインスタンスの固有の番号およびソフトウエアの内容のハッシュ関数値を有するソフトウエアのインスタンスに関する情報の偽造不能な固有な収集物である。ソフトウエアベンダーは、知的所有権を侵害するソフトウエアの侵害インスタンスを検出する侵害ソフトウエア検出機構を有する。ソフトウエアベンダーは、ソフトウエアの侵害インスタンスを保護センターに送ることにより、使用管理はソフトウエアの侵害インスタンスの使用の試みを検出する。

【００９２】

本発明の他の実施形態として、テスト中で装置の識別子と一体となったソフトウエアの少なくとも１つのインスタンスを作るソフトウエアベンダーが提供される。上記のテストは、代表的なプログラミング言語の中の“ＩＦ文”である。上記テストは、一体となった識別子とソフトウエアインスタンスが使用される装置の識別子とを比較する。一体化した識別子が装置の識別子と等しい時に、ソフトウエアインスタンスは正常に使用できる。等しくなければ装置上の管理プログラムにより報復措置が実行される。さらに、保護手段を追加する為にソフトウエアインスタンスのハッシュ関数値のデジタル署名（一体化した識別子を有する）が送られ、第２テストはデジタル署名が真正であるか否かを判断し、第３テストは署名された値がソフトウエアインスタンスのハッシュ関数値と同じであるか否かを判断する。同じでない時、装置内の管理プログラムにより報復措置が実行される。

【００９３】

上記において述べたように、ユーザー装置は、ソフトウエアのインスタンスを受け取り、ソフトウエアのインスタンスに固有に関連付けられたタグを安全に受け取り、そしてソフトウエアのインスタンスにアクセスするようにユーザー装置のユーザーからの試みを受け取る入力部を有する。ユーザー装置のプロセッサは、保護プログラムを実行する。保護プログラムは、ソフトウエアのインスタンスのアクセスの試みを検出し、ユーザー装置のユーザーによるソフトウエアのインスタンスへのアクセスを許可する前にソフトウエアのインスタンスに関連付けられたタグが真正であるかを判断する。保護プログラムは、呼び出し手順が呼び出しポリシーに従っているようにリクエストされているかを判断し、タグテーブルに格納されたタグのステータスを更新するように、呼び出し手順を実行する。呼び出し手順中に、保護プログラムは、タグテーブルをユーザー装置からユーザー装置に結合された相互接続機構を介して送り、タグテーブルの各タグに対して実行される動作を示すユーザー装置へ戻る継続メッセージの受け取りを待つ。この方法で、ユーザー装置は、使用管理ポリシーのセッティングに関係する必要がなく、単にすべての装置に対して中央集中的なポリシーを保持するだけでよい。

【００９４】

ユーザー装置にインストールされたタグのないソフトウエアのインスタンスに対し、保護プログラムはタグのないソフトウエアのインスタンスを検出し、タグのないソフトウエアのインスタンスに指紋処理を実行し、ユーザー装置の指紋テーブルにおける指紋処理から得られた指紋を格納する。タグのないソフトウエアに対しては、呼び出し手順中に保護プログラムは、ユーザー装置からの指紋テーブルをユーザー装置に結合された相互接続機構を介して送信し、ユーザー装置に格納されたタグのないソフトウエアのインスタンスに対して実行される動作を示すユーザー装置に戻される継続メッセージの受け取りを待つ。

【００９５】

タグのないソフトウエアに対しては、保護センターにおける確認プログラムはタグのないソフトウエアのインスタンスの指紋を受け取るために呼び出し手順を相互接続機構を介して定期的に実行する。確認プログラムは、受け取った各指紋を指紋データベースを用いて検査することにより、タグのないソフトウエアのインスタンスがソフトウエアの侵害インスタンスであるか否かを判断し、侵害インスタンスである場合には、確認プログラムはユーザー装置に対して報復措置を生成する。確認プログラムが指紋データベースと受け取った指紋中の１つとの一致を検出した場合には、確認プログラムは実行される報復措置を特定し、確認プログラムは継続メッセージをユーザー装置に送る。継続メッセージは、それを受け取るユーザー装置に行う報復措置を示す。

【００９６】

本発明の他の実施形態は、ソフトウエアのインスタンスを受け入れ、ソフトウエアのインスタンスに付き１つのタグの割合で複数のタグを作る真正証明サーバーを提供する。各タグは、関連付けられたソフトウエアのインスタンスを固有に識別し、各タグはタグに関連付けられたソフトウエアのインスタンスの名称に関する符号化された情報、タグに関連付けられたソフトウエアのインスタンスの固有の番号およびタグに関連付けられたソフトウエアのインスタンスで算定されたハッシュ関数値を有する。

【００９７】

ソフトウエアへのアクセスを管理する方法において、ソフトウエアのインスタンスを作るステップが実行される。次にソフトウエアのインスタンスに固有に関連付けられたタグが作られる。ソフトウエアのインスタンスおよびタグが次にユーザー装置に配布される、上記の方法は、次にユーザー装置においてソフトウエアのインスタンスへのアクセスの試みを検出し、ソフトウエアのインスタンスへのアクセスの試みが、アクセスされるソフトウエアのインスタンスに関連付けられたタグのステータスを判断することによって有効であるか否かを判断する。

【００９８】

タグを作るには、上記の方法は固有の番号をソフトウエアのインスタンスに割り当て、ソフトウエアのインスタンスの内容に関する第１ハッシュ関数値を算定する。第２ハッシュ関数値は、ソフトウエアのインスタンスに対して算定される。第２ハッシュ関数値は、ソフトウエアの名称、ソフトウエアのインスタンスの固有の番号、ソフトウエアのインスタンスの内容および第１ハッシュ関数値を有する。最後に、上記の方法は、ソフトウエアのインスタンスに固有に関連付けられるタグを算定する。タグは、ソフトウエアの名称、ソフトウエアのインスタンスの固有の番号および第２ハッシュ関数値を有する。

【００９９】

タグを算定するステップは、署名ハッシュ関数値を作る第２ハッシュ関数値のデジタル鍵署名関数を適用し、タグに署名ハッシュ関数値を有することにより、デジタル的に署名されたタグを作る。これにより、タグの配布を安全にする。公開鍵暗号化技法は、タグをソフトウエアベンダーおよびユーザー装置に安全に配布するのに使用できる。

【０１００】

ソフトウエアはユーザー装置のソフトウエアインスタンスを入手し、ユーザー装置におけるソフトウエアインスタンスに関連付けられたタグを安全に入手することによって配布できる。ユーザー装置は、ソフトウエアのインスタンスに関連付けられたタグが署名されているか否かを判断し、署名されている場合にはタグの署名ハッシュ関数値を確認でき、署名ハッシュ関数値が確認されると、ユーザー装置はソフトウエアをインストールすることができる。

【０１０１】

ユーザー装置におけるソフトウエアのインスタンスへのアクセスの試みを検出するために、本発明の方法は、ソフトウエアのインスタンスへのアクセスに対するユーザーのリクエストを阻止するように、ユーザー装置に保護プログラムを作動させるステップを有する。ソフトウエアのインスタンスへのアクセスへの試みが有効か否かを判断するために、上記の方法は、呼び出しポリシーに基づいて呼び出し手順が必要であるか否かを判断する。上記の方法は、真正であることを確認し、ソフトウエアのインスタンスに関連付けられたタグの使用ポリシーを判断するために、呼び出し手順を実行し、呼び出し手順の結果に基づいてユーザー装置におけるタグ情報を更新する。タグに関連付けられたステータス情報がユーザー装置で検査されることにより、タグに関連付けられたソフトウエアのインスタンスへのアクセスが有効であるか否かを判断する。この方法で、ソフトウエアの保護が行われる。

【０１０２】

呼び出し手順中に、ソフトウエアのインスタンスに関連付けられたタグを格納するタグテーブルは、ユーザー装置から送られる。上記ユーザー装置はタグテーブルにおける各タグに対して実行される動作を示すユーザー装置に戻される継続メッセージの受け取りを待つ。

【０１０３】

保護センターは、ソフトウエアのインスタンスに関連付けられたタグを有するタグテーブルを受け取り、タグテーブルに受け取られた各タグをタグ付きのソフトウエアデータベースを用いて検査することにより、タグテーブルの中のタグが少なくとも一つの使用管理ポリシーに一致することを確かめる。保護センターは、各タグに関連付けられたソフトウエアのインスタンスへのアクセスの試みを検出した後にユーザー装置が続行する動作を示す継続メッセージを送る。

【０１０４】

本発明の他の実施形態は、上記の処理に対して指示で符号化された装置読み取り可能媒体を有し、伝播信号は上記の符号化されたタグテーブルデータ構造体を搬送する媒体を通じて搬送波を介して送られる。

【０１０５】

これらの機構を用いることにより、本発明のシステムは、ソフトウエアのインスタンスにおける正当な権利を有するベンダー／オーナーの権利を保護取り締まる。ベンダーのソフトウエアと実質的に同じであるソフトウエアのインスタンスが密造され、盗まれ、リバースエンジニアリングされ、改変され、または解体されたことを発見することによって、ベンダーに対する権利侵害をベンダーが発見する場合には、システムはソフトウエアの不正コピーの使用を取り締まる。

【０１０６】

本発明のシステムは、同時にソフトウエアの正当な権利を有するユーザー／オーナーによるソフトウエアについて不正使用の偽りの印象を作り出そうと試みる不正なグループによるサービスの拒絶から、ソフトウエアの正当な権利を有するユーザーを保護する。

【０１０７】

本発明は、また使用ごとに支払われるソフトウエアに対する各ユーザー装置において、使用ごとの支払い統計値が追跡される。呼び出し手順中、保護センターは、ソフトウエアの使用ごとの支払いインスタンスに対する使用統計値を判断し、費用請求のためにソフトウエアベンダーに使用情報を送る。

【０１０８】

上述したように、上記システムは、タグ付きソフトウエアデータベースおよび確認プログラムを持つ保護センターを有する。各ユーザー装置は、呼び出し手順を介して保護センターと定期的に通信し、ユーザー装置にインストールされ、または前の呼び出し手順から装置に用いられているベンダーソフトウエアの各インスタンスに対して、そのインスタンスに関連付けられたタグを安全に送る。タグテーブルからの追加データは、完全なタグテーブルを有するまで、呼び出し手順中に保護センターに管理プログラムによって安全に送られる。呼び出し手順は、保護センターまたはユーザー装置により初期化される。保護センターの確認プログラムは、ユーザー装置から受け取る各タグの真正を証明する。

【０１０９】

本来、確認プログラムは、タグ付鍵のソフトウエアデータベースを用いてユー

ザー装置から受け取った各タグおよび関連付けられたデータを検査することにより各タグの真正を証明し、タグが関連付けられたソフトウエアインスタンスに適用される少なくとも１つの使用管理ポリシーに適合することを確認する。例えば、確認プログラムは、呼び出し中に受け取ったタグが同じ管理プログラムから前の呼び出し時に、コール装置のタグテーブルにおける使用可能な状態、そして同時にその他の装置のタグテーブル使用可能な状態で、使用確認ポリシーの違反の出現があったか否かをチェックする。確認プログラムは、継続メッセージをユーザー装置に安全に戻し、呼び出し手順中に受け取られたタグおよび関連付けられた情報を用いてタグ付きソフトウエアデータベースを更新する。

【０１１０】

ソフトウエアのインスタンスに対して署名されないタグを作る時、タグサーバーはタグを保護センターに安全に送り、保護センターの確認プログラムは受け取ったタグをタグ付きソフトウエアデータベースに格納する。

【０１１１】

他の実施においては、タグサーバーはすべての新しく作られたタグを保護センターに送り、保護センターの確認プログラムは受け取った各タグをタグ付きソフトウエアデータベースに格納する。保護センターが呼び出し手順中にユーザー装置からタグを受け取る時に、保護センターの確認プログラムは、タグを保護センターのタグ付きソフトウエアデータベースの中で検索することによって、タグの真正を証明し、発見できない場合には、そのタグが署名されていないタグであって真正でないことを表す。上記のタグが署名されたタグであれば、確認プログラムは、タグをタグ付きのソフトウエアベース中に発見するか、または上記のタグが正しい形状を持ち、タグの中にデジタル署名を有することを確認するかによって、タグの真正を証明する。

【０１１２】

ユーザー装置への保護センターの継続メッセージは、保護センターにより署名され、タイムスタンプ、タグテーブルのハッシュ関数値、または呼び出し中にユーザー装置の管理プログラムから受け取った他のデータのハッシュ関数値のような識別データを有する。更に継続メッセージは、ユーザー装置の管理プログラム

に対するコマンド（以下、コール動作と呼ぶ）を有する。

【０１１３】

本発明により用いられる措置例は、以下の事項を含むが、これらに限定されるものではない。

管理プログラムが、（１）特定のソフトウエアインスタンスの継続使用を可能にすること、（２）指定された時間内、ソフトウエアインスタンスの使用を拒絶すること、（３）指定された時間内、所定の名称または所定の指紋リストを有するソフトウエアのインストールまたは使用許可を拒絶すること、または（４）指定された時間内、ユーザー装置の機能を停止することを、指示する。

【０１１４】

呼び出し手順中に保護センターから継続メッセージを受け取ると、ユーザー装置の管理プログラムが保護センターのデジタル署名をチェックする。管理プログラムは、さらに、継続メッセージが本装置の現呼び出しのためのものであるかを、継続メッセージ中に存在するハッシュ関数値または他のデータと、本装置におけるタグテーブルの一部のハッシュ関数値もしくはタグテーブルのハッシュ関数値またはタグテーブル中に存在する他のデータと比較することによってチェックする。

【０１１５】

前記署名は認証されたものであることが確認され、前記比較の結果が一致していると認められると、管理プログラムは現呼び出し手順中に、保護センターの回答として継続メッセージを受け入れる。この場合、管理プログラムは、継続メッセージをタグテーブルに格納し、タグの状況を更新し、前記措置に従ったメッセージ中の措置および前記継続報復措置を実行する。

【０１１６】

使用管理ポリシーは、ソフトウエアインスタンスの個別のタグ、特定のソフトウエアもしくはソフトウエアタイプ、保護センターが通信する全てのユーザー装置、または保護センターが通信するユーザー装置の個別のユーザーに関連付けられることができる。

【０１１７】

ソフトウエアインスタンスのベンダーによって決められる使用管理ポリシーの例は、以下に示すとおりであるが、これらまたはこれらの組み合わせに限定されるものではない。あるユーザー装置で一旦用いられたソフトウエアインスタンスは、別のユーザー装置では使用されない。あるソフトウエアインスタンスは、同時に２つのユーザー装置で使用されることがないか、または使用可能な状況ではない。あるソフトウエアインスタンスは、特定の装置セットのユーザー装置のみにおいて同時に使用され、または使用可能な状況である。あるソフトウエアインスタンスは、特定回数よりも多く使用されないものとする。あるソフトウエアインスタンスは、特定日付の後には使用されない。あるソフトウエアインスタンスの使用は、そのインスタンスに対するペイパーユーズ（使用ごとに支払う）料金が特定口座に振り込まれた時にのみ、許される。

【０１１８】

本発明にかかる方法および装置は、ソフトウエアインスタンス、またはソフトウエアインスタンスのクラスの使用に関して、ベンダーまたはベンダー協会によって決められた使用管理ポリシーの遵守を可能にする。

【０１１９】

保護センターは、ユーザー装置におけるソフトウエアインスタンスに関連した個別のタグに対するタグ付きソフトウエアデータベース中に、タグデータ構造体を保持する。タグに対するタグデータ構造体は、タグ自体に関連付けられ、呼び出し手順中に保護センターにそのタグを転送したユーザー装置に関連付けられるわけではない。各タグデータ構造体は、ソフトウエアインスタンスのタグ、インスタンスがそのコピーであるソフトウエアの名称、ソフトウエアインスタンスのインスタンス番号、ソフトウエアインスタンスもしくはその一部のハッシュ関数値、ソフトウエアインスタンスに関連した使用管理ポリシー、および呼び出し記録の参照の収集物、またはソフトウエアインスタンスに関連した呼び出し記録収集物を備える。前記呼び出し記録収集物の各呼び出し記録は、ある呼び出し手順に関する情報を示す。この呼び出し記録は、また、呼び出し時刻、呼び出し手順中に保護センターに転送されるタグテーブルヘッダのような識別情報、先行の呼び出し手順のタイムスタンプが示す前回呼び出し時刻、呼び出し手順中に保護セ

ンターに伝送されるタグテーブルのハッシュ関数値、および呼び出し手順中にユーザー装置の管理プログラムに送信される継続メッセージを有してもよい。

【０１２０】

呼び出し手順中に収集されて格納されたデータを用いて、保護センターは、ソフトウエアインスタンスのペイパーユーズに対する請求書を作るために、各ソフトウエアインスタンスの使用統計を編集することができる。

【０１２１】

タグのないソフトウエアインスタンスが、ユーザー装置でインストールまたは使用されてもよい。管理プログラムは、インスタンスにタグがないことを検出し、タグのないソフトウエアインスタンスの選ばれた部分の指紋を算定し、ユーザー装置の指紋テーブルにこれらの指紋を格納する。この構成にかかる保護センターは、指紋データ構造体を有する。ユーザー装置による上述の呼び出し手順中に、保護センターは、ユーザー装置にインストールされたタグのないソフトウエアインスタンスごとに、ユーザー装置から全ての指紋を受け取る。確認プログラムは、ユーザー装置から受け取った各指紋を指紋データ構造体における指紋と対比することによって、ユーザー装置で用いられているタグのないソフトウエアインスタンスが権利侵害のソフトウエアインスタンスであるかを判定する。この方法によって、本発明は、タグが除去されたベンダーソフトウエアの権利侵害の複製であるソフトウエアインスタンス、またはベンダーソフトウエアの権利侵害から派生した派生物であるソフトウエアインスタンスの使用を検出することができる。

【０１２２】

保護センターの指紋データ構造体の特定数よりも多い指紋とユーザー装置から受け取った指紋とが一致していることを確認プログラムが検出すると、確認プログラムは、ユーザー装置に戻す継続メッセージに報復措置を記すことができる。このような報復措置の一つによれば、保護センターによってタグのない権利侵害のソフトウエアを用いていることを検出されると、このユーザー装置は指定期間、機能を停止させられる。

【０１２３】

別の例では、保護センターの指紋データ構造体の指紋に一致した指紋に関連したタグのないソフトウエアインスタンスの機能は停止される、と報復措置が記してもよい。

【０１２４】

権利侵害ソフトウエアがタグのないソフトウエアとして配布され、または使用されていることを、ソフトウエアベンダーが検知して、このようなタグのないの権利侵害ソフトウエアの複製を保護センターに送ることによって、保護センターの指紋データ構造体は構築される。保護センターは、この権利侵害ソフトウエアの複製の一部についての指紋を算定し、これらの指紋を指紋データ構造体に格納する。

【０１２５】

ベンダーのソフトウエア権利侵害の防止は、また、タグの有無にかかわらず、ユーザー装置で用いられたソフトウエアインスタンスの選ばれた部分の指紋を作り、これらの指紋をこの装置の指紋テーブルに格納することによっても可能である。上述のように、指紋テーブルの指紋は、呼び出し手順の実行中にユーザー装置の管理プログラムによって保護センターに送られ、保護センターの確認プログラムは、受け取った指紋と保護センターの指紋データ構造体の指紋との間の一致を調べる。本発明のこの構成は、正当なベンダーのソフトウエアの権利侵害バージョンを作ってこの権利侵害ソフトウエアのタグ付きインスタンスを配布する権利侵害ベンダーによって、正当なベンダーの権利が侵害されるのを防止する。

【０１２６】

装置読み取り可能媒体上の符号化されたタグテーブルデータ構造体を、ユーザー装置はアクセスできる。タグ付きソフトウエアがこの装置にインストールされ、またはこの装置によって使用されると、タグテーブルデータ構造体は、一つのソフトウエアインスタンスに固有に関連した少なくとも一つのタグを有し、タグテーブルのタグに関連した少なくとも一つの領域を有する。この領域は、タグに関連した一つのソフトウエアインスタンスの使用管理状況を示し、タグに関連した一つのソフトウエアインスタンスの使用統計をも示す。タグテーブルデータ構造体は、また、タグテーブルを一意に識別し、このタグテーブルを一つのユーザ

ー装置または一つのユーザー装置の管理プログラムに一意に関連付けるタグテーブルヘッダを有してもよい。タグテーブルヘッダは、ユーザー装置の使用統計に関する情報および継続メッセージを有する。継続メッセージは、タグに関連したソフトウエアインスタンスに対する可能な措置および使用管理状況を示す。

【０１２７】

ソフトウエアベンダーは、名称およびソフトウエアの内容を有するソフトウエアインスタンスを作り出すソフトウエア開発工程を提供する。ベンダーの各ソフトウエアインスタンスは、このソフトウエアインスタンスに関連した固有のタグと共でなければアクセスまたは使用が可能とならない。タグは、関連するソフトウエアインスタンスに関する、偽造が不可能な固有の情報収集物であり、ソフトウエアの名称、ソフトウエアインスタンスの固有の識別番号およびソフトウエアの内容の一部のハッシュ関数値を有する。ソフトウエアベンダーは、また、ベンダーの知的所有権などを侵害するソフトウエアインスタンスを検出する侵害ソフトウエア検出機構を備える。ソフトウエアベンダーが権利侵害のソフトウエアインスタンスの複製を保護センターに送ることによって、権利侵害のソフトウエアインスタンスの使用およびアクセスの企てを検出し、検出すると、このソフトウエアインスタンスを有するユーザー装置に報復措置を課すように、本発明の方法は保護センターによって用いられる。

【０１２８】

ユーザー装置は、ソフトウエアインスタンスを受け取り、ソフトウエアインスタンスに一意に関連したタグを安全に受け取る入力ポートを有する。ユーザー装置は、また、このソフトウエアインスタンスのインストールまたは使用の要求を受ける。ユーザー装置のプロセッサが管理プログラムを実行する。管理プログラムがソフトウエアインスタンスのインストールまたは使用の試みを検出し、このソフトウエアインスタンスのインストールまたは使用を許可する前に、このソフトウエアインスタンスに関連したタグが認証されたものであること、またはタグに関連した状況を確認する。管理プログラムは、呼び出しポリシーによって決められているように、時々、呼び出し手順が必要であることを決定し、タグテーブルに格納されているタグの状況を更新するために、管理プログラムが呼び出し手

順を実行する。

【０１２９】

呼び出し手順中、管理プログラムはユーザー装置に結合された相互接続機構を介してユーザー装置からのタグテーブルを安全に送り、ユーザー装置に戻されてくる、タグテーブルのタグごとに実行されるべき措置を示す継続メッセージの受け取りを待つ。この方法により、ユーザー装置は使用管理ポリシーの設定に関して配慮する必要がなく、全ての装置に共通な使用管理ポリシー、またはベンダーによって配布されるソフトウエアインスタンスに関連したベンダーの使用管理ポリシーを遵守するだけでよい。

【０１３０】

ユーザー装置の管理プログラムによって実施される呼び出しポリシーは、この装置、この装置で用いられる特定のソフトウエアインスタンス、またはこの装置の特定のユーザに関連付けられてもよい。呼び出しポリシーの例は、以下のものを含むが、これらに限定されるわけではない。ユーザー装置の次の呼び出し時刻は、前回の呼び出しからの経過時間、前回の呼び出し以降の装置起動回数および前回の呼び出し以降に装置が使用された全時間の組み合わせによって求められてもよい。同様に、タグ、またはこのタグに関連したソフトウエアインスタンスに関連した呼び出しポリシーが、前回の呼び出しからの経過時間、ソフトウエアインスタンスが使用された回数およびソフトウエアインスタンスがこの装置で用いられた全時間の関数として、次の呼び出し時刻を求めてもよい。ソフトウエアインスタンスに関連した別の呼び出しポリシーは、ユーザー装置においてソフトウエアインスタンスの使用が試みられる度に、呼び出しを実行することを記してもよい。

【０１３１】

本発明は、呼び出しポリシーによって指定された次の呼び出し時刻以前に、保護センターを呼び出して継続メッセージを保護センターから受け取るのを怠った場合に特定の報復措置を管理プログラムに実行させることによって、前記ユーザー装置または前記ユーザー装置のタグテーブルのタグに適用される呼び出しに適合するように、ユーザー装置およびその管理プログラムを動作させる。前記メッ

セージが実際に前記呼び出し用の継続メッセージとして保護センターによって送られる場合に限り、ユーザー装置の管理プログラムがこの呼び出しに対する保護センターの継続メッセージとして、呼び出し手順の実行中に、受け取ったメッセージを受け入れることを本発明は保証する。これは、上述のように、保護センターがこの継続メッセージに署名し、ユーザー装置の管理プログラムによる現呼び出しに一意にリンクした識別データをこのメッセージに含めること、および保護センターが前記署名および前記識別データを確認することによって達成される。呼び出しポリシーに従った保護センターの呼び出しを行わないことや、不正な継続メッセージを作成もしくは使用する企てによって、ユーザーまたはユーザー装置が本発明の保護の対象から外れてしまうのを、本発明のこの構成要素が防止する。

【０１３２】

呼び出しポリシーを適合するのに怠った際に前記装置の管理プログラムによって実行されるユーザー装置の前記報復措置の例は、以下の事項を含むが、これらに限定されるわけではない。管理プログラムは、呼び出し手順の実行を除いて、指定期間装置を機能停止させてもよい。ソフトウエアインスタンスに関連した呼び出しポリシーが違反されると、装置がこのソフトウエアインスタンスの使用を指定期間停止してもよい。

【０１３３】

ユーザー装置でインストールまたは使用される、タグのないソフトウエアインスタンスに対して、管理プログラムは、タグのないソフトウエアインスタンスを検出し、タグのないソフトウエアインスタンスに指紋処理を実行し、この指紋処理から得られた指紋をユーザー装置の指紋テーブルに格納する。タグのないソフトウエアに対して、呼び出し手順中、管理プログラムは、相互接続機構を介してユーザー装置からの指紋テーブルを保護センターに送り、保護センターからユーザー装置への継続メッセージの受け取りを待つ。このメッセージは、ユーザー装置に格納された、タグのないソフトウエアインスタンスごとに、実行されるべき措置を示す。

【０１３４】

タグのないソフトウエアに対して、ユーザー装置の管理プログラムは、タグのないソフトウエアインスタンスの指紋を相互機構を介して送るために、呼び出し手順を定期的に実行する。この呼び出し手順は、ユーザー装置の管理プログラムまたは保護センターによって初期化されてもよい。保護センターの確認プログラムは、受け取った各指紋を保護センターの指紋データ構造体と対比して調べることにより、このタグのないソフトウエアインスタンスが権利侵害のソフトウエアインスタンスではあるかを判定する。権利侵害のソフトウエアインスタンスであれば、確認プログラムは、ユーザー装置に対する報復措置を準備する。例えば、確認プログラムが、指紋データ構造体における特定ソフトウエアに関連した指紋と、ユーザー装置のタグのないソフトウエアに関連した指紋との間に、十分な数の一致を検出すると、確認プログラムは実行されるべき報復措置を記して継続メッセージをユーザー装置に送信する。継続メッセージを受け取るユーザー装置において実行されるべき報復措置を、継続メッセージは示す。

【０１３５】

前記タグサーバーは、一般に、特定ソフトウエアのコピーを受け入れ、前記ソフトウエアインスタンスごとに固有のタグを複数生成する。各タグは、関連したソフトウエアインスタンスを一意に識別する。各タグは、また、タグに関連したソフトウエアインスタンスの名称と、タグに関連したソフトウエアインスタンスの固有番号と、ソフトウエアの前記名称、ソフトウエアインスタンスの前記固有番号、およびタグに関連したソフトウエアの内容を算定したハッシュ関数値を組み合わせたハッシュ関数値とに関する情報を備える。

【０１３６】

ソフトウエア使用の管理方法において、ソフトウエアインスタンスを作るステップは、上述のように実行される。次に、ソフトウエアインスタンスに一意に関連したタグが作成される。ソフトウエアインスタンスおよびタグが、次に、ユーザー装置に配布される。次に、ソフトウエアインスタンスのユーザー装置における使用の試みが検出され、使用されるべきソフトウエアインスタンスに関連したタグの状況を判定されることで、ソフトウエアインスタンスのこの使用の試みが、許可されるものであるかが判定される。

【０１３７】

タグを作るために、本方法は、ソフトウエアインスタンスに固有番号を割り当て、ソフトウエアインスタンスの内容の第１ハッシュ関数値を算定する。次に、本方法は、ソフトウエアの名称、ソフトウエアインスタンスの固有番号、および第１ハッシュ関数値を組み合わせた第２ハッシュ関数値を算定する。最後に、本方法は、ソフトウエアインスタンスに一意に関連したタグを形成する。このタグは、ソフトウエアの名称、ソフトウエアインスタンスの固有番号および前記第２ハッシュ関数値を含む。

【０１３８】

タグを作るステップは、さらに、タグに含まれる前記第２ハッシュ関数値にデジタル署名関数を適用し、署名されたハッシュ関数値をタグに含めることによって、デジタル的に署名されたタグを生成することができる。

【０１３９】

ソフトウエアインスタンスおよびソフトウエアインスタンスに関連したタグをユーザー装置に取得させることによって、ソフトウエアが配布されてもよい。ユーザー装置は、ソフトウエアインスタンスに関連したタグに署名されていることを判定し、署名されていれば、タグのハッシュ関数値およびタグにされた署名確認する。この確認が成功すれば、ユーザー装置はソフトウエアインスタンスをインストールまたは使用することができる。

【０１４０】

ユーザー装置のソフトウエアインスタンスへのアクセスの試みを検出するために、本発明のこの方法は、ソフトウエアインスタンスの使用のユーザー要求を遮るように、ユーザー装置の管理プログラムに訴えるステップを有する。ソフトウエアインスタンスの使用の試みが有効であると判定するために、本方法は、呼び出し手順が呼び出しポリシーに基づいて必要とされているかを判定する。本方法は、呼び出し手順を実行して、認証されたものであることを確かめ、ソフトウエアインスタンスに関連したタグの使用管理ポリシーを決定する。本方法は、また、この呼び出し手順の結果に基づいて、ユーザー装置におけるタグ情報を更新する。タグに関連した状況情報はユーザー装置で調べられて、タグに関連したソフ

トウエアインスタンスの使用が許容されるものであるかが判定される。この方法において、ソフトウエアの使用管理が可能となる。

【０１４１】

呼び出し手順中、ソフトウエアインスタンスに関連したタグを格納するタグテーブルは、ユーザー装置から保護センターに安全に送られ、ユーザー装置は、タグテーブルの各タグに対して実行されるべき措置を示す、ユーザー装置に戻される継続メッセージの受け取りを待つ。

【０１４２】

保護センターは、ソフトウエアインスタンスに関連したタグを含むタグテーブルを受け取り、タグテーブルの受け取られた各タグをタグ付きのソフトウエアデータベースに対比して調べ、タグテーブルのタグが少なくとも一つの使用管理ポリシーに従っていることを保証する。保護センターは、各タグに関連したソフトウエアインスタンスの使用の試みを検出すると、ユーザー装置が従うべき措置を示す継続メッセージを送信する。

【０１４３】

本発明の別の実施形態は、前記処理の指示で符号化されたコンピュータ読み取り可能媒体と、上述のようにタグテーブルデータ構造体を安全に搬送する媒体上を搬送波によって送られる伝搬信号とを有する。

【０１４４】

これらの機構を用いて、本発明のシステムは、ソフトウエアインスタンスにおける権利の正当なベンダー／オーナーがこれらの権利を警備することを可能にする。ベンダーによって製造されたソフトウエアと基本的に同一動作を行う、密造され、盗まれ、逆行分析され（プログラムを解析され）、または改変されたインスタンスを発見するなどして、ベンダーの権利が侵害されていることをベンダーが発見すると、このシステムは、ソフトウエアのこれら違法コピーの使用を取り締まることができる。

【０１４５】

本発明のシステムは、同時に、正当なユーザーによるソフトウエアの使用が違法であるという誤った印象を作り出そうとする不正者によって、サービスが拒絶

されてしまうことがないように、ソフトウエアの正当なユーザーを保護する。

【０１４６】

本発明は、また、使用ごとを基礎として購入されたソフトウエアインスタンスに対する各ユーザー装置におけるペイパーユーズ統計の追跡を可能にする。呼び出し手順中、保護センターは、ソフトウエアインスタンスのペイパーユーズ用の使用統計を求めることができ、料金請求のために使用情報をソフトウエアベンダーに送り返すことができる。

【０１４７】

【発明の実施の形態】

本発明の前記および他の目的、特徴および利点は、図面に示すように、本発明の好ましい実施形態の説明から明らかであり、前記図面はその全体を通じて同一部品には同一符号が用いられている。図面における寸法は正確ではなく、本発明の原理を示すのに重点が置かれている。

【０１４８】

図１は、本発明に従って構成された情報システム１０９の一例を示す。図１には、本発明の主要な構成要素が記載され、本発明に動作上の関係を有するものも記載されている。情報システム１０９は、複数のユーザー装置１０４～１０７と、一つ以上のソフトウエアベンダー１０１、一つ以上のタグサーバー１０２および一つ以上の保護センター１０３とを相互通信する通信ネットワーク１００を有する。なお、本実施形態では、ソフトウエアベンダー１０１、タグサーバー１０２および保護センター１０３は、それぞれ、一つだけ示されている。本発明は、ユーザー装置が、ある情報のオーナー、配布者またはベンダーの知的所有権または他の権利を侵害して、その情報をインストールまたは使用するのを防止するように、ユーザー装置１０４～１０７の一つによって用いられる情報の使用を管理するもの（図示せず）である。

【０１４９】

知的所有権または他の権利を保護するために、本発明によって使用が管理される情報は、電子的、磁気的、光学的などで表現された、いかなるタイプのものであってもよい。情報の例として、コンピュータソフトウエアアプリケーションす

なわちプログラム、データ、ウエブページもしくはウエブサイト、例えばＪａｖａ（登録商標）アプレットのようなダウンロード可能なアプリケーションプログラム、コンパクトディスク、磁気ディスク、テープ等に記録された電子ブック、画像、ビデオ、音楽などの情報がある。一般に、例えばユーザー装置１０４～１０７のようなコンピュータまたは他の装置によって用いられる、あらゆるタイプの情報の使用が管理され、この情報が何であるか、またはこの情報が格納または伝送される実際の物理媒体が何であるかには関係なく、この情報に関する権利は本発明によって保護される。

【０１５０】

このような情報、および本発明による保護が可能な当業者によって認識されている情報を、以下ではソフトウエアと称する。例えば特定のアプリケーションプログラム、または特定のブックもしくはビデオのコピーのような特定のソフトウエアの個別のコピーを、以下ではソフトウエアのインスタンス、またはソフトウエアインスタンスと称する。ソフトウエアのオーナー、ベンダーまたは配布者を、以下ではベンダーまたはソフトウエアベンダーと称する。装置を使用して、または装置上で、ソフトウエアインスタンスをインストール、使用、実行、読み取り、表示、演奏、鑑賞、印刷、複製、伝送またはアクセスすることを、以下ではそのソフトウエアインスタンスの使用と称する。

【０１５１】

ユーザー装置１０４～１０７は、ソフトウエアの使用に用いられ、これらに限定されるものではないが、コンピュータシステム、ブックリーダ、例えばテーププレーヤ、コンパクトディスクプレーヤ、ミニディスクプレーヤのようなミュージックプレーヤ、ビデオカセットレコーダ、デジタルビデオディスク（ＤＶＤ）プレーヤ、専用装置などを含むあらゆるタイプの装置である。これらの装置を、以下ではユーザー装置または単に装置と称する。

【０１５２】

本発明の好ましい実施形態では、ユーザー装置（すなわち１０４～１０７のいずれか）はコンピュータシステムであり、前記情報はコンピュータアプリケーションプログラムもしくはデータである。本発明は、このソフトウエアに関するベ

ンダーの権利を保護するように、コンピュータシステムのユーザーによるソフトウエアもしくはデータの使用を管理する機構を提供する。

【０１５３】

通信ネットワーク１００は、本発明の構成要素（１０１～１０７）がメッセージまたは信号のような情報を交換するのを可能にする、あらゆるタイプの接続機構である。通信ネットワーク１００の例として、インターネット、公衆交換電話網（ＰＳＴＮ）、無線ネットワーク（すなわちセルラーネットワーク）、または他のタイプのコンピュータもしくは情報ネットワークのようなコンピュータネットワークがある。

【０１５４】

本発明の一般的な運用によれば、一つ以上のソフトウエアベンダーのうちのソフトウエアベンダー１００が、ソフトウエアインスタンス（図１には示さず）を作成し、配布する。ソフトウエアインスタンスは、各ユーザー装置１０４～１０７で使用されるために、装置１０４～１０７でインストールまたは使用される。例えば、ソフトウエアがテープの音楽であれば、テープは図１でテーププレーヤとして図示されているユーザー装置１０５にインストールされる。ソフトウエアは、ソフトウエアベンダー１０１から物理的または手動的に搬送され、ユーザー装置１０４～１０７に物理的なテープの場合のようにインストールされるか、または公知のデータ伝送機構、すなわちソフトウエアベンダー１０１からユーザー装置１０７にソフトウエアのインスタンスをダウンロードする場合のような機構を用いて、ソフトウエアは通信ネットワーク１００を介して電子的に伝播されてインストールされる。

【０１５５】

通信ネットワーク１００に結合されたコンピュータシステムであるタグサーバー１０２は、各ソフトウエアインスタンスに対してタグ（図１には示さず）を作成すなわち生成する。通常、特定のソフトウエアの全てのインスタンスは同一である。好ましくは、一つのタグは、ソフトウエアベンダー１０１によって作成された一つのソフトウエアインスタンスに一意にに関連している。タグサーバー１０２は、ソフトウエアベンダー１０１によって作成されたソフトウエアに、好ま

しくは独自の通信経路１０８を介してアクセスする。タグは、好ましくはソフトウエアの内容、ソフトウエアの名称、および例えばインスタンス番号のようなタグサーバーによって生成された情報やベンターによって提供された情報などの他の情報に基づいて生成される。タグサーバー１０２は、また、通信ネットワーク１００を用いて、タグを付すためにソフトウエアを取得することもできる。

【０１５６】

代わりに、各種ソフトウエアの多様なインスタンスを販売する一つのソフトウエアベンダー１０１が存在してもよい。このソフトウエアベンダー１０１に対して、一つのタグサーバー１０２および一つの保護センター１０３が存在してもよい。タグサーバー１０２および保護センター１０３は、ソフトウエアベンダー１０１の一部であってもよく、すなわち同一コンピュータシステム内に含まれてもよい。代わりに、一つ以上の共有タグサーバー１０２および共有保護センター１０３に依存してサービスを受けるソフトウエアベンダー１０１の協会が存在してもよい。

【０１５７】

タグがソフトウエアインスタンスに対して作成されると、このタグに対応するソフトウエアインスタンスがインストールされているユーザー装置１０４～１０７の一つに、このタグは安全に伝播される。安全なタグの伝播は、好ましくは、例えば安全な通信のためのＴＥＴＳ　ＩＰＳＥＣやＮＥＴＳＣＡＰＥ　ＳＳＬプロトコルの使用によって、通信ネットワーク１００を介して電子的に行われる。手動による安全なタグの伝播も、本発明のシステムによって用いられる。手動による安全なタグ伝播の一例として、タグおよび可能ならば関連したソフトウエアインスタンスを含む、改変されないパッケージ内でタグを配布する。

【０１５８】

ソフトウエアのインスタンスおよびソフトウエアインスタンスに関連したタグがユーザー装置１０４～１０７に一旦インストールされると、この装置のユーザー（図示せず）またはこの装置自体は、このソフトウエアの使用を試みることができる。しかし、ソフトウエアインスタンスの使用が許可される前に、ユーザーまたはソフトウエアを有するユーザー装置１０４～１０７によって要求されたソ

フトウエアインスタンスに対する有効なタグがこの装置内に存在することを、このユーザー装置の管理プログラム（図示せず）が確認する。定期的に、各ユーザー装置が保護センター１０３と通信ネットワーク１００を介して通信する。これにより、ユーザー装置上のソフトウエアインスタンスに関連した全てのタグが、有効であることおよび使用管理ポリシーに従って用いられていることが保証される。

【０１５９】

すなわち、本発明は、ソフトウエアインスタンスの装置による使用が、有効な関連タグの存在にリンクされていることを保証する。タグは、ユーザー装置を保護センターに通信させることによって、使用特性が定期的に確認およびをチェックされる。遵守される使用管理ポリシーの例では、タグは一つの装置にのみ存在する。ユーザー装置１０４～１０７がソフトウエアインスタンスを使用することができるか否かの判定は、ユーザー装置と保護センター１０３との間で実行される後述の呼び出しと呼ばれるタグ処理手順に基づく。

【０１６０】

本発明にかかる実施形態のさらに詳細な説明を行う前に、以下の表１（表１Ａ～表１Ｃから構成される）に、本発明に関連する各種の要素の理解を助けるための用語集を示す。

【０１６１】

【表１Ａ】

表１Ａ：用語の定義（その１）

用語	定義
ACTIONS(措置)	装置で使用してもよいソフトウエアを記載し、検出されたベンダーソフトウエアの不正使用に対する報復措置を記す継続メッセージCMに含まれる措置指令。
CALL-UP_POLICY_SW (呼び出しポリシー)	特定のソフトウエアSWまたは特定のソフトウエアインスタンスINST_SWに関連付けられ、任意に指定された呼び出しポリシーであって、装置が何時保護センターに呼び出し手順を実行しなければならないかを規定する。
CM(継続メッセージ)	保護センターからユーザー装置に送られる継続メッセージであって、ユーザー装置のソフトウエアインスタンスの使用許可状況を示す。
DEVICE IDENTIFIER (装置識別子)	ハードウエア識別子から、または管理識別子ID(SP)を用いることによって、装置を識別する方法。この識別は、各ソフトウエアインスタンスがテストにおいて装置識別子を組み込む実施形態で用いられる。
FP(X) (指紋)	入力ストリングＸに指紋関数（例えばハッシュ関数）を施して算定される指紋。
GC	保護センター。
HASH_INST_SW	HASH_SW,NAME,NUM_INST_SWおよび他の領域から算定されるハッシュ関数値。
HASH_SW	ソフトウエアSWの内容から算定されたハッシュ関数値。各ソフトウエアインスタンスSWは同一のHASH_SWを有する。HASH_SWはHASH(SW)の他の表記である。HASH_SWは、ソフトウエアの一部のみのハッシュ関数値結果の場合もある。
ID(X), ID(SP)	オブジェクトXに任意に関連付けられた固有の識別番号。例えば、ID（管理プログラム）は、起動イベントが起きた時点と、保護センターによって提供される情報および一つ以上のメモリ位置の値を含む他の情報とを組み合わせることによって、最初に装置が起動した際に算定された管理プログラムの識別番号である。

【０１６２】

【表１Ｂ】

表１Ｂ：用語の定義（その２）

INF_SW (権利侵害のソフトウエア)	ベンダーによって確立された知的所有権または他の権利を侵害する、ベンダーのソフトウエアSWの認証されていない複製または派生物。権利侵害のソフトウエアの配布を検出し、このソフトウエアの権利侵害的な使用を防止する法律上の権利を、ベンダーが持つこととする。権利侵害のソフトウエアには、タグが不適切な方法で除去されたもの、タグが変更されたもの、または装置識別テストがある場合にこれが変更されたものが含まれる。
INST_SW （インスタンス）	ソフトウエアSWの全インスタンスセットから選ばれた特定のソフトウエアの特定のインスタンス（複製またはコピー）。ソフトウエアSWの全てのインスタンスは同一である。
NAME_SW	特定のソフトウエアSWの名称。
NUM_INST_SW （インスタンス番号）	特定のソフトウエアインスタンスINST_SWに関連付けられた固有番号。この番号は、数字、アルファベット、文字もしくは記号が混ざった列、または他のパターンである。同一の原則が上記識別ID(X)に適用される。
POLICY(TAG_INST_SW) または USAGE SUPERVISION POLICY （使用管理ポリシー）	知的所有権およびアクセス権の保護、またはソフトウエアに関連付けられたペイパービュー（観るごとに支払う)使用制限に関するソフトウエアベンダーまたは他の組織によって規定されたポリシーおよび規制。これらポリシーおよび規制は、特別のソフトウエアインスタンスに依存してもよい。POLICY(TAG_INST_SW)は、保護センターGCおよび管理プログラムSPによって遵守される。
SP, SUPERVISING PROGRAM	管理プログラム。ユーザー装置に一体化されたプログラムであって、本明細書に記載されている、ユーザー装置のソフトウエアインスタンスの使用管理を行うメカニズムを提供する。
PRIVATE_KEY_X	デジタル的な署名を生成するためのXによって用いられる秘密鍵。
PUBLIC_KEY_X	署名をチェックして認証するために、Xによってデジタル的に署名されることが意図された、データの受領者によって用いられる公開鍵。
SIGN_TS（署名）	タグサーバのデジタル署名。

【０１６３】

【表１Ｃ】

表１Ｃ：用語の定義（その３）

SIGN_X(M)	メッセージMのXによるデジタル的な署名であって、以下の特性を有する。(1)Xのみが SIGN_X(M)を生成することができる。（2）デジタル的な署名の受領者は、XがMを署名していることを確認できる。
SPARSE_SET（疎セット）	疎で秘密の番号セットであって、一実施形態においては、この番号セットから固有のインスタンス番号が全てのソフトウエアインスタンスに選ばれる。インスタンス番号は物理的処理によって生成されてもよい。
SPARSE_SET_SW（疎セット）	疎で秘密の番号セットであって、一実施形態においては、この番号セットから固有のインスタンス番号NUM_INST_SWが一つの特定のソフトウエアSWのインスタンスに選ばれる。これにより、ソフトウエアXのインスタンスはソフトウエアYのインスタンスと同一のインスタンス番号を持つことができる。インスタンス番号は物理的処理によって生成されてもよい。
SW（ソフトウエア）	本発明によって保護される特定のベンダーソフトウエアである。例えばスプレッド(Spread)という名称のソフトウエアコードがある。
TAG_INST_SW	偽造が不可能な固有の署名がされているか、または署名されていないタグであって、特定のソフトウエアインスタンスINST_SWに関連付けられている。
TAG TABLE（タグテーブル）	ソフトウエアインスタンスに関連付けられたタグに関する情報と、装置のソフトウエアインスタンスの使用または使用管理に関する情報とを含む装置に格納されたテーブルまたはファイル。
UNTAGGED_SW（タグのないソフトウエア）	関連付けられたタグTAG_SWを持たず、ユーザーがユーザー装置でインストールまたは使用することを試みるソフトウエア。例えば、シェアウエアもしくはフリーウエアまたはユーザーによって作成されたソフトウエアである。
ＶＲＰ（確認プログラム）	保護センターGCにおける確認プログラム。

【０１６４】

技術用語の詳細な定義：

本発明の一定の実施形態は、本質的に複雑である。したがって、本発明の一定の実施形態によって用いられる技術用語に対する、他の補助的な定義を以下に示す。

１．指紋関数またはハッシュ関数Ｆ：ＸとＹが等しくなければ、Ｆ（Ｘ）とＦ（Ｙ）が等しくない可能性が高くなるように、データＸを、より小さいデータＦ（Ｘ）に対応づけるで数学的関数。ハッシュ関数の例として、Ｘはバイト列であ

る。さらに、好ましくは、数値ｐはランダムに選ばれるが、以後は固定された６４ビットの素数である。バイト列Ｘは、ある数値（２５６ベースで書かれ、バイトはその数値の数字である）およびＦ（Ｘ）＝Ｘ　ｍｏｄ　ｐ（Ｘをｐで割った余り）と見なされる。これにより、Ｆ（Ｘ）の値は、Ｘがいかに大きくても６４ビットストリングである。

２．偽造できないハッシュ関数Ｈ：所定のＸに、Ｈ（Ｘ）を算定するのは容易であるが、Ｈ（Ｘ）＝Ｈ（Ｘ’）かつＸとＸ’は異なるような、Ｘ’を生成するのが困難な性質を有する指紋関数。用語「困難」は、現在の技術水準によればＸのサイズでは必要な演算時間が一般に指数関数的であるか、または事実上実現不能であると一般に理解されることを意味する。偽造できないハッシュ関数の例として、ＭＤ５がある。

【０１６５】

３．ソフトウエアインスタンスの使用：装置の使用によって、または装置において、ソフトウエアインスタンスの、インストール、使用、実行、ラン、接続、読み取り、記憶媒体の検索、または記憶媒体の内容変更、表示、演奏、鑑賞、印刷、複製、伝送またはアクセス。

４．ソフトウエアインスタンス部分は、ソフトウエアインスタンスのテキストもしくはデータの全て、またはテキストもしくはデータの一部のシーケンスを含む。

５．指紋処理：データアレーの位置シーケンスが与えられた際における、これらの位置の値に対する関数値の算定。例えば、位置１６，３２および６４が、それぞれ、値３，４および１７を持つ場合、指紋処理は、３，４および１７の関数値を算定する。この関数は、単にこれらの値のリスト（この例では３つの数値）、またはこれらの値のリストのハッシュ関数である。別の例では、位置は、ｉ＿１～ｊ＿１，ｉ＿２～ｊ＿２，…ｉ＿ｋ～ｊ＿ｋであってもよい。指紋処理は、アレーのこれらkシーケンスごとにハッシュ関数値を算定し、ｋ個の算定値をリストに挙げる。

【０１６６】

６．指紋検査：２つの指紋シーケンスを比較する方法。本発明は、２種類の指

紋検査を用いる。２種類の検査は、同一位置指紋検査と一般位置指紋検査である。両方の指紋検査において、指紋リストは、位置リストの一つのリストにおける値に基づいて算定される。例えば、リストに３つの指紋ｆ１、ｆ２およびｆ３があり、ｆ１は位置１０、２０、３０および４０の値から算定され、ｆ２は位置３０および６０の値から算定され、ｆ３は位置１００および２００の値から算定されるとする。このリストを送信リスト（Ｓｅｎｄ　Ｌｉｓｔ）と称することとする。両方の指紋検査において送信リストの受信者は、送信者と同一の指紋リスト位置における値に基づいて指紋リストを算定する。この指紋リストは、受信リスト（Ｒｅｃｅｉｖｅ　Ｌｉｓｔ）と呼ばれる。

同一位置指紋検査では、送信リストの各要素が受信リストの該当する要素に等しい場合に、一致したと宣言される。具体的には、送信リストの第１要素が受信リストの第１要素に等しく、送信リストの第２要素が、受信リストの第２要素に等しく、他の要素についても同様となる。

一般位置指紋検査では、位置に関係無く、送信リストおよび受信リストに多数の共通要素がある場合に、一致したと宣言される。この多数は、ポリシーおよび指紋が作られるデータテキストの長さに依存する。この長さはパラメータｋと定義される。ｋが例えば５０バイトであれば、保護センターの指紋データ構造体（図９の符号１３７）のリストと同一のソフトウエアを装置リスト（Ｄｅｖｉｃｅ　Ｌｉｓｔ）があらわすためには、一つまたは少数の一致で十分である。さらに、一定の一致には他の一致よりも重点が置かれ、重点が置かれていれば少ない一致でも十分である。

指紋の送信リストを送るのに加えて、送信者は、送信リストを生成した値を有する位置リストのリストを送ってもよい。これにより、指紋の計算は、予測し得ないランダム処理に依存する。

【０１６７】

７．偽造不可能：ベンダーの要求に基づいてタグを生成するタグサーバー１０２（図１）によって用いられる秘密情報を知ることなしに、有効なタグを生成するのは、敵対者にとって計算上不可能な場合、タグは偽造不能である。本発明では、デジタル署名（図３Ａ）および疎セット（図３Ｂおよび３Ｃ）を、タグの偽

造不可能を達成する２つの好ましい方法として用いる。

８．安全な伝送：Ｘが転送されるネットワークプロトコルを観察すること、またはＸを転送するパッケージを見ることを他者もできるが、意図された受取人のみがＸを見ることができるような値Ｘを送る方法。信頼できる宅配業者によって配達される封印された包みは、包みの中身を安全に送る一方法である。安全な通信のためのＴＥＴＳ　ＩＰＳＥＣやＮＥＴＳＣＡＰＥ　ＳＳＬプロトコルの使用によってメッセージを送ることは、通信ネットワーク１００（図１）上の安全な伝送を保証する別の方法である。

９．事象履歴：全ての使用の試み、成功した使用、使用期間、および／またはタグテーブルに関連した起動のようなその他の事象の経時的な記録である。２つの装置が、たとえ同一のソフトウエアインスタンスおよび同一の識別子を有していても、同一事象履歴を有することはありそうもない。事象履歴は、一人以上のユーザーよる特定の装置の使用の経時的な記録に基づいてもよい。

【０１６８】

図を用いた説明に戻る。図２には、本発明に従って構成されたシステム１０９のアーキテクチャーの詳細を示す。図２を、本発明の全動作の総合的な記載の概説に用いる。この説明全体を通して、本発明の各構成のより詳細な部分の記載には、他の図が参照される。

【０１６９】

システム１０９の動作において、ソフトウエア（ＳＷ１、ＳＷ２、ＳＷ３、ＳＷ４とされている）のインスタンス（ＩＮＳＴ＿ＳＷ）１１１～１１４は、ソフトウエアベンダー１０１によって作成され、ベンダーストレージ１１０（記憶装置）に格納される。一つ以上のソフトウエアベンダー１１０が存在してもよい。ソフトウエアベンダー１０１の例としては、出版社（複製可能なパフォーマンスの記録、または電子的に読み取り可能な本を作成）、コンピュータソフトウエア開発者（コンピュータソフトウエアアプリケーションプログラムを作成）、データ収集会社（情報データベースを作成）、個人プログラマ等がある。ソフトウエアベンダー１０１によって生成されるソフトウエア（ＳＷ）は、情報、データまたはコードを含む実際のソフトウエアの内容（ＳＷ）を意味する。ソフトウエア

（ＳＷ）は、関連した名称（ＮＡＭＥ＿ＳＷ）を有してもよく、この名称は通常ソフトウエアベンダー１０１によって割り当てられる。ソフトウエアの各インスタンス（ＩＮＳＴ＿ＳＷ）１１１～１１４は、名称を持つソフトウエア（ＳＷ）の別個の物理的な複製（コピー）として考えられる。すなわち、特定のソフトウエア（ＳＷ）に対する各ソフトウエアインスタンス（ＩＮＳＴ＿ＳＷ）は、同一の名称（ＮＡＭＥ＿ＳＷ）および同一のコード、データまたは他の情報内容を持つソフトウエア（ＳＷ）のコピーに過ぎない。

【０１７０】

例えば、文書作成アプリケーションプログラムがソフトウエアベンダー１０１によって作成され、名称（ＮＡＭＥ＿ＳＷ）に「ライト（Ｗｒｉｔｅ）」が与えられるならば、ライトプログラムを備えたバイナリまたは実行可能なコード、データまたは他の情報が、ソフトウエア（ＳＷ）と呼ばれる。ライトソフトウエア（ＳＷ）の個別のコピー（例えば、プログラムのコピーを含む各ディスク）はこのソフトウエアの別個のインスタンス（ＩＮＳＴ＿ＳＷ）であるが、同一のソフトウエア内容（ＳＷ）を持つ。したがって、図２において、各インスタンス１１１～１１４は同一のソフトウエア内容（ＳＷ）を含んで各インスタンス１１１～１１４は同一の名称（ＮＡＭＥ＿ＳＷ）を持つか、または各インスタンス１１１～１１４は異なったソフトウエア（ＳＷ）（すなわち異なったデータ、コードまたは他の情報）のコピーを示し、異なったソフトウエア内容（ＳＷ）を持つ各インスタンスの名称（ＮＡＭＥ＿ＳＷ）１１１～１１４は通常異なる。

【０１７１】

タグサーバー（ＴＳ）１０２は、ベンダー１０１の要求に応じて、各ソフトウエアのインスタンス１１１～１１４用の偽造が不可能な固有のタグ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）１２０を作成する。本発明の好ましい実施形態では、一つの固有のタグは、一つのソフトウエアインスタンスに対して準備され、このインスタンスに関連付けられる。別の実施形態では、複数の固有のタグが一つのソフトウエアインスタンスに関連付けられることはあるが、好ましくは、２つの異なるソフトウエアインスタンスが共通の関連タグを共有することはない。

【０１７２】

要求されたタグを作成するために、ＴＳ１０２（図１）は、作成しようとするタグのインスタンスに対する各特定ソフトウエアのコピーを取得する（図３Ａ、３Ｂおよび３Ｃのステップ１５０）。例えば、ＴＳは、「ライト７．２」の一つのコピーを有してもよい。ここで、「ライト７．２」は、プログラムファミリーライトのリリースすなわちバージョンである。一般に、タグ１０２は、特定のソフトウエアインスタンス（ＩＮＳＴ＿ＳＷ）（すなわち１１１～１１４の一つ）に関連した、偽造が不可能で固有のデータビットシーケンスである。後述するように、本発明の実施形態によれば、ユーザー装置１０４は、ソフトウエアインスタンス１１１～１１４に関連した有効なタグ１２０を最初に調べることなしに、ソフトウエアインスタンス１１１～１１４を使用することはできない。

【０１７３】

ソフトウエアインスタンス１１１～１１４用のタグ１２０は、好ましくは、ストレージ装置２００のタグテーブル２１０に格納される。ストレージ装置２００は、ユーザー装置１０４に結合されているか、またはユーザー装置１０４と一体となっている。ソフトウエアインスタンス１１１～１１４は、タグテーブル２１０に格納されているソフトウエアインスタンス（１１１～１１４の一つ）に関連したタグ１２０を引用し、このタグ１２０が使用状況を持つ場合にのみ、ユーザー装置１０４で用いられることができる。タグの状況としては、例えば図６のタグテーブルの第２列に、「使用状況」が示されている。すなわち、一定のソフトウエアは、このソフトウエアのインスタンスにタグが存在する時にのみ、ランできる、という表示を有する。（侵害者は、この表示を除去するかもしれないが、この場合、後述するタグのないソフトウエアに対する保護機構が適用される。）このようにして、本発明の構成は、ユーザー装置１０４に存在するソフトウエアインスタンスに特に関連した有効なタグを要求することによって、一定の実施形態におけるソフトウエアの使用の権限を許可して与える。

【０１７４】

さらに後述するように、タグの作成、タグの確認およびタグの実施を追跡および管理するために、本発明に従って構成されたシステムの構成部分の能力は、ソフトウエア使用権限に対して、従来のシステムよりも固有の利点を提供する。図

２のシステム１０９のまだ説明をしていない構成部分について説明する前に、タグ作成について詳述する。

【０１７５】

図３Ａ、３Ｂおよび３Ｃは、本発明に従って構成されたタグサーバー１０２におけるタグ作成処理中に行われる処理ステップの好ましい実施形態を示すフローチャートである。これらの図は、互いに似ているので、ステップ番号の多くは同一であり、以下これらの図について同時に説明する。

【０１７６】

ステップ１５０において、タグサーバー１０２は、ローカルストレージから名称を持つソフトウエア（ＮＡＭＥ＿ＳＷ、ＳＷ）のコピー１１１～１１４を取得する。このソフトウエアは、タグが付されるものである。さらに、タグサーバー１０２は、ベンダー１０１からタグ要求（図２）を取得する。ステップ１５１Ａ（図３Ａ），１５１Ｂ（図３Ｂ）および１５１Ｃ（図３Ｃ）において、タグサーバー１０２は、固有番号（ＮＵＭ＿ＩＮＳＴ＿ＳＷ）を生成する。図３Ａのステップ１５１Ａでは、番号は単に固有である。しかし、図３Ｂのステップ１５１Ｂおよび図３Ｃの１５１Ｃでは、固有番号（ＮＵＭ＿ＩＮＳＴ＿ＳＷ）は疎セット１１８（図２）から選ばれる。

【０１７７】

疎セット１１８（図２）は秘密番号のセットであって、この秘密番号のセットから名称を持つソフトウエア（ＮＡＭＥ＿ＳＷ、ＳＷ）のインスタンスそれぞれに対してインスタンス番号（ＮＵＭ＿ＩＮＳＴ＿ＳＷ）が選ばれる。好ましくは、利用可能な番号の範囲（例えば、特定のソフトウエアに１億のインスタンスが存在し、６４ビットにより定められる範囲においては１００億以上の可能な番号が存在する場合）に比較して、前記番号の数は比較的少ない。したがって、セット１１８は、疎（sparse：散在する、まばらな）と称される。

【０１７８】

疎であることより、敵対者または侵害者にとって、有効なインスタンス番号を生成するのは困難である。全てのソフトウエアに対して一つの疎セットが存在してもよい。または、関連したインスタンスのセットにより決められた各特定のソ

フトウエアに対して、それぞれ異なる疎セットが存在してもよい。好ましい実施形態では、一つの疎セット１１８が、全てのソフトウエアに対するインスタンス番号の源として用いられる。しかし、各特定のソフトウエアに対して別の疎セット１１８を持つことによって、より単純なインスタンス番号生成の配布管理を可能にしてもよい。

【０１７９】

例えば、上述の「ライト」アプリケーションソフトウエアに関連した疎セット番号１１８（ＳＰＡＲＳＥ＿ＳＥＴ＿ＳＷ）が存在してもよい。この疎セット番号１１８から、ライトソフトウエアの各インスタンス（ＩＮＳＴ＿ＳＷ）に対してインスタンス番号（ＮＵＭ＿ＩＮＳＴ＿ＳＷ）が選ばれる。安全上の理由から、疎セットの新しい番号は、要求があり次第、例えば光電計数装置（本発明では図示せず）のような物理的処理へのアクセスによって、実現または生成されてもよい。

【０１８０】

ステップ１５２（図３Ａおよび３Ｂ）において、タグサーバー１０２は、ソフトウエア（ＳＷ）の内容またはその内容の一部についてハッシュ関数値を算定する。好ましい実施形態において、同一ソフトウエア内容ＳＷを有する２つ以上のソフトウエアインスタンス（ＩＮＳＴ＿ＳＷ）１１１～１１４にタグが付されている場合、ハッシュ関数値ＨＡＳＨ＿ＳＷがソフトウエア（ＳＷ）に対して１回だけ算定される。これは、各インスタンス１１１～１１４が同一のコード、情報および／またはデータを含む、すなわち同一のＳＷ内容を持つからである。さらに、値ＨＡＳＨ＿ＳＷは、全てのソフトウエアのコピーごとに検索または生成されるよりも、タグサーバー１０２によって１回検索または生成されるだけを必要とする。本発明のこの構成は、同一ソフトウエア（ＳＷ）の多くのインスタンスにタグを付す際には、タグ作成時間を節約する。このような場合、ハッシュ関数値ＨＡＳＨ＿ＳＷの算定の必要性は１回限りである。別の実施形態では、ソフトウエア内容の一部のみについてのハッシュ関数値の算定によって、さらに最適化される。これは、タグサーバー１０２とユーザー装置１０４～１０７の両者におけるハッシュ関数値の確立に必要な時間が、さらに減少するからである。

【０１８１】

ステップ１５３（図３Ａ、３Ｂおよび３Ｃ）においてソフトウエアインスタンス（ＩＮＳＴ＿ＳＷ）に関連したタグに組み込まれる第２ハッシュ関数値ＨＡＳＨ＿ＩＮＳＴ＿ＳＷが算定される。ステップ１５３は、ステップ１５２とは異なる。ステップ１５２において算定されたハッシュ関数値ＨＡＳＨ＿ＳＷは同一ソフトウエアＳＷのすべてのインスタンスＩＮＳＴ＿ＳＷに対して同一であるのに対し、ステップ１５３においてはハッシュ関数値ＨＡＳＨ＿ＩＮＳＴ＿ＳＷが同一ソフトウエアＳＷの各ＮＵＭ＿ＩＮＳＴ＿ＳＷに対して固有である。一実施形態では、第２ハッシュ関数値ＨＡＳＨ＿ＩＮＳＴ＿ＳＷは、ソフトウエアの名称（ＮＡＭＥ＿ＳＷ）、ソフトウエアインスタンスの固有番号（ＮＵＭ＿ＩＮＳＴ＿ＳＷ）およびステップ１５２で既に算定されたハッシュ関数値ＨＡＳＨ＿ＳＷを共に組み合わせる。名称およびソフトウエアのみ、またはソフトウエアおよび番号のみ、などのような他の組み合わせは、当業者には理解される同様の機能を提供するものとして認識される。このようなハッシュ関数を介してエンコードされたデータの組み合わせは、本発明の範囲内に含まれる。

【０１８２】

ハッシュ値ＨＡＳＨ＿ＩＮＳＴ＿ＳＷがソフトウエア１１１～１１４の各インスタンスに対して算定された後に、署名されたタグ（図３Ａ）または署名されていないタグ（図３Ｂおよび３Ｃ）が、ステップ１５４Ａおよび１５４Ｂによって、これらのインスタンス１１１～１１４に対して作成される。図３Ａのステップ１５４Ａにおいて署名されたタグがソフトウエアインスタンス１１１～１１４に対して作成されるのに対し、図３Ｂおよび３Ｃのステップ１５４Ｂにおいては、署名されていないタグがソフトウエアインスタンス１１１～１１４に対して作成される。準備されたタグのデジタル署名のある部分によって、たとえインスタンス番号が、例えば続き番号であるために予測できる場合であっても、偽造不可能であることを、署名されたタグが保証する。署名されていないタグは、この保証機能を提供することはできないが、ステップ１５４Ｂにおいて生成された署名されていないタグは、好ましくは疎セット１５１Ｂから選ばれたインスタンス番号ＮＵＭ＿ＩＮＳＴ＿ＳＷを含むので、この代わりの方法によって、タグの偽造不

可能が保証される。署名されたタグＴＡＧ＿ＩＮＳＴ＿ＳＷは、ステップ１５４Ａにおいて、以下のように算定される。

TAG_INST_SW=(NAME_SW,NUM_INST_SW,HASH_INST_SW,
SIGN_TS(HASH_INST_SW))

ここで、ＳＩＧＮ＿ＴＳは、ＨＡＳＨ＿ＩＮＳＴ＿ＳＷハッシュ関数値において実行されるデジタル署名関数である。デジタル署名ＳＩＧＮ＿ＴＳは、全ての考えられる敵対者および図２のタグサーバー１０２自体を除いたあらゆる団体（ユーザー装置、ベンダー等）から秘密に保たれているデジタル的な鍵（キー）である秘密鍵（プライベイトキー）ＰＲＩＶＡＴＥ＿ＫＥＹ＿ＴＳ１１７を用いて、タグサーバー１０２によって生成される。

【０１８３】

署名されていないタグＴＡＧ＿ＩＮＳＴ＿ＳＷは、ステップ１５４Ｂ（図３Ｂ）において以下のように算定される。

TAG_INST_SW=(NAME_SW,NUM_INST_SW,HASH_INST_SW)

【０１８４】

タグサーバー１０２によってタグＴＡＧ＿ＩＮＳＴ＿ＳＷが生成された後、タグは、好ましくは、図２のタグ１２０によって示され、図３Ａおよび３Ｂのステップ１５６に関して後述するように、タグを要求するソフトウエアベンダー１０１および保護センター１０３に安全に送られる。保護センター１０３では、図９の符号１２９，１３８に関して後述するように、タグ１２０は各種のタグデータベースに格納される。

【０１８５】

ソフトウエアインスタンス（例えば１１１）に関連したタグ１２０、およびタグ１２０がタグサーバー１０２によって準備される方法は、本発明の多数の重要な目的に合致する。

（１）関連した有効タグ１２０、好ましくは装置（例えば１０４）のタグテーブル２１０（図６に詳細に示されている）に保持されているタグ１２０を装置１０４が格納またはアクセスしない限り、かつ、このタグ１２０が、関連インスタンス１１１の適切な使用を許可または指示するタグテーブル２１０に使用状況（

図６の第２列）を持たない限り、装置１０４はベンダー１０１のソフトウエアインスタンス１１１を使用することはできない。

（２）装置（例えば１０４）と保護センター１０３の間の後述する命令された呼び出し手順（図１２、１３Ａおよび１３Ｂ）によって、保護センター１０３は、タグ属性を管理、認証、追跡、確認および一般的に監督し、タグ１２０に関連したソフトウエアインスタンス１１１が、ソフトウエアインスタンス１１１に対するベンダー１０１の使用管理ポリシーに従って用いられていることを保証する。この使用管理ポリシーは、好ましくは保護センター１０３によって保持されている。

（３）タグ１２０の偽造が不可能で、タグ１２０が好ましくは安全な方法で送られることより、ベンダー１０１（またはタグサーバー１０２）からタグ１２０を合法的に取得し、このソフトウエアインスタンス１１１に対するベンダー１０１の規定された使用管理ポリシー（この図には示さず）に従って関連したソフトウエアインスタンス１１１～１１４を使用するユーザーまたはユーザー装置１０４のみが、このタグ１２０を持つことについて保証される。本発明のこの構成は、敵対者または侵害者が有効なタグ１２０のコピーの生成および／または使用を試みるのを防止する。これにより、本発明の機構によって、コピーする敵対者／侵害者にも、ソフトウエアインスタンス１１１および関連したタグ１２０を用いる合法的なユーザーまたはユーザー装置に対するのと同様に、報復措置を作り出す。

【０１８６】

タグ１２０には、いくつかの別の構成が考えられる。別の構成の一つでは、以下に示すように、フィールドのサブセットを持つ。特に、ハッシュ値ＨＡＳＨ＿＿ＩＮＳＴ＿＿ＳＷはタグ１２０に含めず、ＮＡＭＥ＿＿ＳＷおよびＮＵＭ＿＿ＩＮＳＴ＿＿ＳＷをタグ１２０に残す。このような実施形態の利点は、システム構成要素（例えば１０１、１０２、１０３、１０４）の間で送られ、各タグ１２０について算定されるデータが少ないことである。不利な点は、タグ１２０のオーナーが、異なる特定のソフトウエアインスタンス１１１にタグ１２０を関連させることを試みるかも知れないことである。これは、値ＨＡＳＨ＿＿ＩＮＳＴ＿＿ＳＷがＨＡＳ

Ｈ＿ＳＷに依存し、インスタンス１１１内のソフトウエアＳＷが正しいか、または変更されていないかを確認するために、ＨＡＳＨ＿ＳＷが用いられるので、ＨＡＳＨ＿ＩＮＳＴ＿ＳＷがタグ１２０で利用される際に防止される。

【０１８７】

第２の別のタグ構成は、ＮＡＭＥ＿ＳＷ、ＮＵＭ＿ＩＮＳＴ＿ＳＷ、ＨＡＳＨ＿ＳＷである。この構成を用いることにより、全てのタグ１２０は、その内容（すなわちＳＷ）がＨＡＳＨ＿ＳＷに対するハッシュ関数に一致するソフトウエアに関連される。この方法の不利な点は、正しく見える違法タグ１２０を、侵害者が生成できる可能性があることである。ソフトウエアの使用を保護するために選ばれる本発明の実施形態の複雑性に応じて、本明細書に記載のシステムは、各種の記載した問題を解消するように構成されている。

【０１８８】

別の例として、タグ１２０の第３の別の構成は、ＮＡＭＥ＿ＳＷ、ＮＵＭ＿ＩＮＳＴ＿ＳＷ、ＨＡＳＨ＿ＳＷ、ＳＩＧＮ＿ＴＳ（ＮＡＭＥ＿ＳＷ、ＮＵＭ＿ＩＮＳＴ＿ＳＷ、ＨＡＳＨ＿ＳＷ）である。このタイプのタグ１２０では、デジタル署名がタグの偽造を防止する。これは、好ましくはタグサーバー１０２のみが署名関数ＳＩＧＮ＿ＴＳの演算に必要な秘密鍵ＳＥＣＲＥＴ＿ＫＥＹ＿ＴＳを持つからである。

【０１８９】

取り除かれてもよい別のタグ領域は、領域ＮＡＭＥ＿ＳＷである。この実施形態の利点は、システム構成要素間で送られるデータの量を減らすことである。タグがＩＮＳＴ＿ＳＷをランまたは使用するのに存在しなければならない名称以外の手段によって、ソフトウエアインスタンスＩＮＳＴ＿ＳＷを示すのであれば、名称は不必要となる。名称のないタグは、例えば所定のソフトウエアベンダー１０１から配布されるソフトウエアが１種類しか存在しない場合、ソフトウエアベンダー１０１の識別子は、このベンダーによって生成されたソフトウエアに対する名称として用いられることができる。代わりに、ＮＵＭ＿ＩＮＳＴ＿ＳＷが、全ての種類のソフトウエアを通して固有である場合、ＮＡＭＥ＿ＳＷは不要である。

【０１９０】

タグ１２０から取り除かれてもよい別の領域は、ＮＵＭ＿ＩＮＳＴ＿ＳＷである。このタグ構成の利点は、ネットワーク１００上を送られるデータの量が減少し、固有の番号選択処理（例えば図３Ａ、３Ｂおよび３Ｃに説明されているステップ１５１）を必要とすることなく、より簡単なタグ作成方法を用いることができることにある。不利な点は、同一のＮＡＭＥ＿ＳＷ（この領域が保持されているならば）を持つ、異なるタグの識別ができなくなって、二重のインスタンス１１１～１１４が許容されてしまうことである。

【０１９１】

タグの別構成の他の実施形態は、任意の領域Ａを含む。ＩＤ（ＳＰ）（図４の２０９－Ａ）と表されたユーザー装置（例えば１０４）の管理プログラム（後述する図４の符号２０９）の固有識別子が、例えばハードウエア特定装置、可能ならば装置１０４の管理プログラム２０９が初めて起動された時点、および可能ならば保護センター１０３から装置の管理プログラム２０９によって安全に取得された固有番号と、装置内の少なくとも一つのメモリ位置の値との組み合わせから算定される。これは後に詳述するが、ここでは各種のタグ作成処理の理解のために記述する。ユーザー装置１０４～１０７で用いられるソフトウエアインスタンス１１１に関連したタグ１２０にユーザー装置１０４～１０７の管理プログラム２０９の識別子ＩＤ（ＳＰ）２０９－Ａを含めることで、以下に詳述するように、割安な保護センター１０３呼び出しをサポートすることができる。

【０１９２】

本発明の別のタグおよびタグ作成の実施形態に含まれる任意の領域は、ソフトウエアインスタンスＩＮＳＴ＿ＳＷ内データの特定の位置における指紋リストである。指紋について後述するが、その名称が示唆するように、指紋はソフトウエアインスタンスから選ばれる一部分もしくは複数部分またはデータ領域の固有のエンコードされたものである。指紋の使用方法は、図３Ｃのステップ１５１Ｄおよび１５１Ｅに示されている。ここで、位置が選ばれ、次にこれらの位置における指紋が算定され、その結果に関してハッシュが算定される。インスタンスに関連したタグ１２０内に、ソフトウエアインスタンス１１１の指紋を含めることに

よって、ユーザー装置１０４～１０７における管理プログラム（ソフトウエアのアクセスに用いられる、図４の符号２０９）が、ＩＮＳＴ＿ＳＷとタグの関連付けが正しいことを確認することができる。この関連付けが正しいかは、ＩＮＳＴ＿ＳＷにおいて同一位置指紋検査（詳細な定義は図６による）を行って、関連したタグの指紋リストと比較することによって確認する。指紋の使用がＨＡＳＨ＿ＳＷの関数とオーバーラップしてもよく、これによりタグとソフトウエアインスタンスの関連付けが正しいことの確認には、大きな効果が生じる。

【０１９３】

例えば、百科事典またはビデオのような大きなソフトウエアインスタンスＩＮＳＴ＿ＳＷに対して、管理プログラムによるＩＮＳＴ＿ＳＷの全ての走査を必要とするＨＡＳＨ＿ＳＷの算定には、相当の時間を要する。ＩＮＳＴ＿ＳＷに関連したタグがタグサーバーにより算定される前記固定位置の指紋値を含むと、管理プログラム（図４の符号２０９）はＩＮＳＴ＿ＳＷのこれらの位置にのみアクセスして、該当の指紋値を算定するだけでよい。前記の指紋を用いることによって、追加的な保護上の利点が生じる。これは、タグサーバーによって指紋が算定される位置が、侵害者の権利侵害に応じて、経時点に変化できるからである。

【０１９４】

ソフトウエアＳＷ全体ではなく、ＳＷの特定の部分のみについてタグサーバー１０２によってハッシュ関数値ＨＡＳＨ＿ＳＷが算定される（図３ＡおよびＢのステップ１５２）ならば、同様の効率および安全性が得られる。タグサーバー１０２によって指紋が算定されたソフトウエアインスタンスＩＮＳＴ＿ＳＷ１１１～１１４における特定の位置は、タグ１２０内に指紋を明示的に伴うか、またはインスタンスＩＮＳＴ＿ＳＷもしくは装置１０４～１０７の管理プログラム（図４の符号２０９）に含めてもよい。タグ１２０にこれら指紋位置を用いることの利点は、送られるインスタンスＩＮＳＴ＿ＳＷごとに、指紋が変化でき、指紋は固有のＮＵＭ＿ＩＮＳＴ＿ＳＷの一種として用いられ、ソフトウエアコードが変更していることのランダムチェックを可能にすることである。

【０１９５】

したがって、以下の領域組み合わせからなるタグ１２０は、全て本発明の範囲

内に含まれる。；図３Ａ、３Ｂおよび３Ｃの処理結果として生成されるタグ。；前記の組み合わせのいずれかに、ＩＤ（ＳＰ）のようなユーザー装置（例えば１０４）に対する管理プログラム識別子２０９－Ａ（図４）を加えたもの。ただし、ＩＤ（ＳＰ）の値は、ハッシュ関数値ＨＡＳＨ＿ＩＮＳＴ＿ＳＷの算定に組み合わされる。；前記の組み合わせのいずれかに、ソフトウエアＳＷの内容に関連した指紋リストを加えたもの。ただし、これらの指紋の値は、ハッシュ関数値ＨＡＳＨ＿ＩＮＳＴ＿ＳＷの算定に組み合わされる。；前記の領域の組み合わせのいずれかの上位セット。前記のタグおよび処理の記述は、本発明の実施形態の特定の例について記載しているが、当業者には、複数の特定のソフトウエアインスタンスの一つの使用を一意に識別および監督するために、本発明によって提供されていると理解される。

【０１９６】

タグ１２０がソフトウエアインスタンス１１１～１１４に対して作成されると、タグ１２０は、ステップ１５６において、タグサーバー１０２によって保護センターのデータベース（図９の符号１２９，１３８に関して後述される）、ユーザー装置１０４、ソフトウエアベンダー、またはこれら団体の組み合わせに対して安全に送られる。

【０１９７】

図２に戻って、タグ１２０は、タグサーバー１０２によって、一つ以上のソフトウエアベンダー１０１、保護センター１０３およびユーザー装置１０４に安全に配布される。タグ１２０が、タグサーバー１０２によってソフトウエアベンダー１０１には安全に送られるが、ユーザー装置１０４～１０７には送られない場合、ソフトウエアベンダー１０１によってソフトウエアインスタンス１１１～１１４と共に、タグ１２０はユーザー装置１０４～１０７に送られる。別の実施形態では、ソフトウエアインスタンス１１１～１１４は、タグ１２０とは別個にユーザー装置１０４～１０７によって取得される。タグ１２０は、タグサーバー１０２からユーザー装置１０４～１０７によって直接取得される。代わりに、タグ１２０は、一つ以上の保護センターセンタ１０３から取得することができる。

【０１９８】

ソフトウエアのインスタンス１１１～１１４は、安全に配布されることを要求されないが、それらは本発明のシステム１０９の代案実施形態には要求されることがある。ソフトウエアのインスタンス１１１～１１４の配布は、いくつかの方法で行うことができる。インスタンス１１１～１１４は、コミュニケーションネットワーク１００を通じサポートされるダウンローディング機構を介してソフトウエアベンダーからダウンロードすることができる（図１）。ダウンローディング機構の例は、Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ（ＦＴＰ）、情報を受領者に送るＰＵＳＨプロトコル、ＴＣＰ／ＩＰおよびＷｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ関連のプロトコル、ならびにコンピュータープロセッサの間のバスを介してデータを送るために用いられる他のプロトコル、または例えばインターネットを代表とするコミュニケーションネットワーク１００のような他のタイプのコンピューターネットワークである。

【０１９９】

あるいは、ユーザー装置１０４は、ソフトウエアベンダー１０４と同じ固体であることもないこともあり得るユーザー装置メーカー（図示されず）によりあらかじめインストールされるソフトウエアのインスタンス１１１～１１４をあらかじめ備えることができる。例は、ユーザー装置１０４の中のファームウエアに組み込まれたソフトウエアのインスタンス１１１～１１４である。他の代案として、ユーザー装置１０４のユーザー（この図には示されていない）は、ソフトウエアのインスタンス１１１～１１４をユーザー装置により読み取り可能な媒体、例えば磁気的に符号化されたハードディスク、またはフロッピー（登録商標）ディスク、または光学媒体、例えばＣＤ－ＲＯＭ、ＤＶＤディスク、ビデオ、またはオーディオテープ、ホログラフィック格納装置、または情報媒体としての別の媒体を通じて購入することができる。ソフトウエアのインスタンス１１１～１１４を入手するためのユーザー装置１０４～１０７に対する前記の代案のそれぞれにおいて、本発明によれば、ソフトウエアのそのインスタンスを用いるために必要とされる付随タグ１２０がソフトウエアのインスタンスに直接付随するか、または別個に好ましくは安全に前記装置に伝送されることができる。

【０２００】

図２に示されたユーザー装置１０４は、ユーザー装置結合機構２００への結合を含む。ユーザー装置ストレージ２００は、ソフトウエアの各インスタンス１１１～１１４、タグテーブル２１０および指紋テーブル１２６を維持することができる。指紋およびタグテーブル１２６，２１０の目的および詳細は、後述される。

【０２０１】

図４は、本発明により構成されたユーザー装置１０４の好ましい構成を図示する。ユーザー装置１０４は、ユーザー装置ストレージ２００、プロセッサ２０１、メモリ２０２、相互接続機構２０３、入／出力機構２０４を結合するインターナルバス２０６を含む。ユーザー２１３は、ユーザー装置１０４と相互に作用し合う。ユーザー２１３は、好ましくは人間であるが、本発明は、この中に説明されている使用管理が、大きな、人間以外の相互作用環境内の電子要素において実行されるシステムに適用することができる。この図において、ユーザー２１３は、本発明の目的を明確に示すためにソフトウエアのインスタンス１１１～１１４と直接に相互作用していることを示されている。実際には、ユーザー２１３は、プロセッサ２０１のコントロールの下でソフトウエアのインスタンス１１１～１１４との間で直接入出力を行うユーザー入／出力機構２０４と、実際にインターフェースすることができる。

【０２０２】

ユーザー入／出力機構２０４は、キーボード、マウス、マイクロフォン、スピーカ、モニタ、ヘッドアップ、またはバーチャルリアリティーディスプレイ、またはユーザー装置１０４と相互作用するユーザー２１３、または他の機構（すなわち人間ではない）との間に情報を交信するために用いられる他の入／出力装置の１つ以上であることが考えられる。入／出力機構２０４は、またユーザー装置１０４がそれによりソフトウエアのインスタンス１１１～１１４を備える手段として使用されることができる。この場合、入／出力機構２０４は、ＣＤ－ＲＯＭ、またはＤＶＤドライブ、スキャナ、フロッピーディスク、またはユーザーストレージ装置２００、またはメモリ２０２、またはユーザー装置（例えば、１０４）に含まれ、または付随することのできるバッファ（図４には示されていない）

に情報をロードするのに用いることのできる他の機構を含むことができる。

【０２０３】

相互接続機構２０３は、コミュニケーションネットワーク１００にインターフェースするために用いられ、モデム、ネットワークインターフェースカード、ワイヤレスレシーバ、またはコミュニケーションに用いられる装置であることが考えられる。

【０２０４】

ハード、フロッピー、または光学ディスクドライブ、ＲＡＩＤアレー、ファイルサーバー、または他の読み／書き格納機構であることの考えられるユーザーストレージ装置２００は、本発明により用いられる各種の要素およびデータを保持するのに用いられる。特にこの実施形態に図示されたように、ユーザーストレージ装置２００は、ソフトウエアのインスタンス１１１～１１４、タグテーブル２１０、指紋テーブル１２６、管理プログラム２０９（図４）およびカーネル２０８を含むオペレーティングシステム２０７を保持する。この分野で理解されているようなオペレーティングシステム２０７は、ユーザー装置１０４のスタートアップ後に通常メモリ２０２にロードされ、ユーザー装置１０４の各種の要素の総合的動作をコントロールするためにプロセッサ２０１と関連して実行する。あるいは、本発明のオペレーティングシステムおよび要素プロセッサは、本発明を具現化するシステムの構成に組み込むことができる。

【０２０５】

ユーザー装置１０４の例は、パーソナルコンピューター、またはワークステーションである。プロセッサ２０１の例は、Ｉｎｔｅｌベースのプロセッサであり、例えばＣｅｌｅｒｏｎ、Ｐｅｎｔｉｕｍ（登録商標）、ＰｅｎｔｉｕｍII、ＰｅｎｔｉｕｍIII、または８０Ｘ８６ファミリ、またはＳＰＡＲＣベースのＲＩＳＣテクノロジを用いるプロセッサ、またはＭＩＰＳプロセッサである。これらのプロセッサの名称は、代表的なマイクロプロセッサメーカーの商標である場合がある。オペレーティングシステム２０７の例は、Ｗｉｎｄｏｗｓ（登録商標）をベースとするあらゆるオペレーティングシステムで、例えばＷｉｎｄｏｗｓＮＴ、Ｗｉｎｄｏｗｓ９８、Ｗｉｎｄｏｗｓ９５、ＷｉｎｄｏｗｓＣＥ、またはＷ

ｉｎｄｏｗｓ３．１で、すべてＭｉｃｒｏｓｏｆｔ Ｃｏｒｐｏｒａｔｉｏｎ ｏｆ Ｒｅｄｍｏｎｄ，Ｗａｓｈｉｎｇｔｏｎ製であり、またオペレーティングシステム２０７は、例えば（登録商標）ベースのシステムで、例えばＳｕｎ Ｍｉｃｒｏｓｙｓｔｅｍｓ Ｉｎｃ．ｏｆ Ｍｏｕｎｔａｉｎ Ｖｉｅｗ，ＣａｌｉｆｏｒｎｉａからのＳｏｌａｒｉｓである。ユーザー装置１０４の他の実施形態は、カスタム、または組み込まれたオペレーティングシステム２０７をもつ特殊プロセッサ２０１を用いる専用機であることが可能である。この分野の熟練者は、前述のユーザー装置１０４がマイクロプロセッサにより制御されるあらゆるタイプの装置であり得ることを理解すべきである。本発明は、図４に示されたユーザー装置１０４の構成により限定されない。むしろユーザーに対してソフトウエアにアクセスすることのできるあらゆる装置は、本発明の範囲に含まれることを意味している。

【０２０６】

本発明のシステムの使用管理の構成を提供するために管理プログラム（ＳＰ）２０９が設けられ、オペレーティングシステム２０７、タグテーブル２１０、ソフトウエアのインスタンス１１１～１１４および選択的に指紋テーブル１２６（図４）に関連して実行する。管理プログラム（ＳＰ）２０９は、好ましくはオペレーティングシステム２０７とは別個のものであるが、その延長部分であることが可能である。管理プログラム（ＳＰ）２０９は、また好ましくはいずれかのプログラミング言語（例えば、Ｃ、Ｃ＋＋、Ｊａｖａ、Ａｓｓｅｍｂｌｅｒ、または他の言語）で記載され、好ましくはオペレーティングシステム２０７のある機能にインターフェースし、制御するためにオペレーティングシステム２０７により設けられるアプリケーションプログラミングインターフェース（ＡＰＩ）を使用する。あるいは、組み込まれたシステムでは、ユーザー装置１０４の中でユーザー装置１０４、オペレーティングシステム２０７、管理プログラム（ＳＰ）２０９および他のデータおよび／または要素が電子回路を介して組み込まれ、完全に代行され、またはメモリに格納されることができる。

【０２０７】

本発明の好ましい実施形態においてユーザー装置１０４のスタートアップ（す

なわちパワーアップ）するごとにオペレーティングシステム２０７、管理プログラム（ＳＰ）２０９およびタグテーブル２１０は、ユーザーストレージ装置２００からメモリ２０２に読み込まれる。ユーザー装置１０４の最初のスタートアップ時に、好ましくは装置の管理プログラム２０９（図４）に対する識別番号ＩＤ（ＳＰ）２０９－Ａは算定され、安全な位置に格納される。前記の用語集において考察されているこの識別番号２０９－Ａ（テーブル１、ＩＤ（ＳＰ））は、下記のある組み合わせにより算定される：利用可能な場合のハードウエア識別番号；利用可能な場合の保護センター１０３（図２）により提供される番号；および装置１０４の中の高精度タイマー（例えばマイクロセカンド）。本発明のシステムにおいて管理プログラム（ＳＰ）２０９は、ソフトウエアのインスタンス１１１～１１４とオペレーティングシステム２０７との間の使用管理インターフェースとして用いられる。管理プログラム（ＳＰ）２０９により提供される使用管理の動作構成が詳細に説明される前に、ソフトウエアのインスタンス１１１～１１４および付随のタグ１２０のユーザー装置１０４へのインストールが考察される。

【０２０８】

図５は、本発明の好ましい実施形態によるユーザー装置１０４に対するソフトウエアインスタンスＩＮＳＴ＿ＳＷおよび付随のタグＴＡＧ＿ＩＮＳＴ＿ＳＷをインストールするステップを図示する。タグ１２０およびソフトウエアのインスタンス１１１～１１４の両者は、ユーザー入／出力機構２０４によりユーザー装置１０４にロードされることによりインストールされることが可能であり、あるいは相互接続機構２０３によりコミュニケーションネットワーク１００からの受け取りを介して電子的にインストールされることができる。図５におけるステップは、好ましくは本発明の一部として提供される管理プログラム（ＳＰ）２０９コードを実行するプロセッサ２０１により行われる。管理プログラム２０９は、例えばカーネル２０８への延長としてオペレーションシステム２０７に存在することができるか、またはカーネル２０８およびオペレーティングシステム２０７の上の別個の処理として存在し、実行することができる。

【０２０９】

いずれの場合にもユーザー装置１０４（この例においてはパーソナルコンピューターであるが、本発明の手段は、発明の主旨に基づくあらゆる他の装置であることができる）は、図５のステップ２５０における特定の名称をもつソフトウエア（ＮＡＭＥ＿ＳＷ，ＳＷ）のインスタンスＩＮＳＴ＿ＳＷを入手する。ステップ２５１においては、ユーザー装置１０４はステップ２５０において入手される名称のソフトウエアに付随するＴＡＧ＿ＩＮＳＴ＿ＳＷを安全に入手する。ステップ２５２においては、本発明のシステムがタグＴＡＧ＿ＩＮＳＴ＿ＳＷが署名された、または署名されていないタグであるかを確かめる。ステップ２５２は、ＳＩＧＮ＿ＴＳ関数値がタグＴＡＧ＿ＩＮＳＴ＿ＳＷの中にあるかないかを確かめるために受け取ったタグ情報を調べることにより行うことができる。次に管理プログラムは、下記のようにタグおよびソフトウエアのインスタンスへのそれの正しい付随を確かめることを行う。

【０２１０】

本発明の好ましい実施形態においては、図３Ａ、３Ｂ、または３Ｃのステップによりタグサーバー１０２により作り出され、署名されていないタグに対してステップ１５４Ａ（図３Ａ）により、また署名されていないタグに対して１５４Ｂ（図３および３Ｃ）により作り出された内容をもつ。タグＴＡＧ＿ＩＮＳＴ＿ＳＷが署名されたタグであればステップ（図５の２５３）は、管理プログラム（ＳＰ）２０９の一部を行うことにより、ハッシュ関数値Ｖ＝ＨＡＳＨ（ＩＮＳＴ＿ＳＷ）およびハッシュ関数値Ｖ＝ＨＡＳＨ（ＮＡＭＥ＿ＳＷ、ＮＵＭ＿ＩＮＳＴ＿ＳＷ、Ｖ）を算定する。管理プログラム２０９は、次に値ＵをタグＴＡＧ＿ＩＮＳＴ＿ＳＷに見られる値ＨＡＳＨ＿ＩＮＳＴ＿ＳＷと比較する。２つの比較された値が合致しない時にはタグは無効である。値ＵおよびＶが合致すると管理プログラム２０９は、タグサーバー１０２の公開鍵ＰＵＢＬＩＣ＿ＫＥＹ＿ＴＳ（図２の１１６）の使用により、タグＴＡＧ＿ＩＮＳＴ＿ＳＷの中にあるＳＩＧＮ＿ＴＳ（ＨＡＳＨ＿ＩＮＳＴ＿ＳＷ）のデジタル署名を確認する。ＳＩＧＮ＿ＴＳ（ＨＡＳＨ＿ＩＮＳＴ＿ＳＷ）におけるタグサーバーの署名が確認されない時には、タグＴＡＧ＿ＩＮＳＴ＿ＳＷは有効ではない。ステップ２５０において得られた名称のあるソフトウエア（ＮＡＭＥ＿ＳＷ、ＳＷ）のインスタンスがステ

ップ２５３の中でステップ２５１において得られた無効タグＴＡＧ＿ＩＮＳＴ＿ＳＷに付随していることがわかれば、ソフトウエアのインスタンスはステップ２５４において拒絶される。

【０２１１】

タグＴＡＧ＿ＩＮＳＴ＿ＳＷが署名のないタグであれば、ステップ２５７は、署名されたタグの場合に対し前記において用いられた同じステップにより、タグＴＡＧ＿ＩＮＳＴ＿ＳＷの中にあるハッシュ関数値ＨＡＳＨ＿ＩＮＳＴ＿ＳＷに対するハッシュ値を確認するために、管理プログラム（ＳＰ）２０９の一部を実行する。ＨＡＳＨ＿ＩＮＳＴ＿ＳＷ値が正しく判定されない時には、タグＴＡＧ＿ＩＮＳＴ＿ＳＷにエラーがあり、無効タグＴＡＧ＿ＩＮＳＴ＿ＳＷに付随するステップ２５０において得られる名称のあるソフトウエア（ＮＡＭＥ＿ＳＷ、ＳＷ）のインスタンスは、ステップ２５４において拒絶される。

【０２１２】

ステップ２５４における拒絶は、ユーザー装置１０４がステップ２５０および２５１において得られたソフトウエアＩＮＳＴ＿ＳＷのインスタンスおよびその付随のタグＴＡＧ＿ＩＮＳＴ＿ＳＷの廃棄、または除去、または使用を許さないことを、単に意味することができる。ステップ２５６もまた実行されることにより、ユーザー装置（例えば１０４）に報復措置を働かせる。ユーザー装置１０４に対する報復措置は、装置をその後停止し、または機能停止することを含むことができる。報復措置は、この発明の使用管理機能に関してさらに詳しく考察される。

【０２１３】

ハッシュ関数値および署名ＳＩＧＮ＿ＴＳ（ＨＡＳＨ＿ＩＮＳＴ＿ＳＷ）は、署名されたタグに対してステップ２５３において確認される時、または署名されていないタグに対してハッシュ関数値ＨＡＳＨ＿ＩＮＳＴ＿ＳＷがステップ２５７において確認される時には、タグに付随するソフトウエアのインスタンスＩＮＳＴ＿ＳＷ（図２の１１１～１１４）をユーザーストレージ装置２００に格納し、またタグにステータス“ＩＮＳＴＡＬＬＥＤ”を取り付けられたタグテーブル２１０にソフトウエアのインスタンス（例えば１１１）に対する付随のタグＴＡ

Ｇ＿ＩＮＳＴ＿ＳＷを格納する（後に詳述されるように、図６に詳細に示されたテーブル２１０の第１欄に）。

【０２１４】

タグがその中で管理プログラム識別番号ＩＤ（ＳＰ）２０９－Ａを含む代案実施形態において、管理プログラム２０９は、タグ１２０の中の管理プログラム識別番号２０９－Ａがユーザー装置１０４に格納された管理プログラム識別番号２０９－Ａと同じであることを確かめる。タグ１２０がその中でソフトウエア内容ＳＷの特定の位置に基づく指紋リストを含む代案実施形態において、管理プログラム２９０は、指紋がソフトウエアＳＷにおける同じ特定の位置において計算された指紋と合致することを確かめ、前記の合致は前記の規定に記載され、この中で詳しく説明されているように同じ位置の指紋に基づいている。

【０２１５】

図６は、凡例としてのタグテーブル２１０の内容を図示している。一般にタグテーブル２１０は、ユーザー装置１０４のユーザー２１３、または装置１０４自体がソフトウエアのインスタンス１１１～１１４の使用を許されているかの決定を行うために管理プログラム（ＳＰ）２０９により要求される情報を含む。後述する処理により管理プログラム２０９は、ソフトウエアのインスタンス１１１～１１４の使用の試みを検出することが可能であり、要求されるインスタンス１１１～１１４に付随するタグＴＡＧ＿ＩＮＳＴ＿ＳＷに対する使用管理特性を求めるためにタグテーブル２１０に保持される情報をチェックすることができる。

【０２１６】

定期的に管理プログラム（ＳＰ）２０９は、ユーザー装置１０４を保護センター１０３（図２）とインターフェースさせる呼び出し手順を実行する。呼び出し手順中、呼び出しを行っているユーザー装置１０４にインストールされたソフトウエアの各インスタンス１１１～１１４に対するタグテーブル２１０のタグ情報は、保護センター１０３（図２）の確認プログラム（図９の３１５）により確認されることにより、ユーザー装置１０４の管理プログラム２０９に、ユーザー２１３が使用を要求しているソフトウエアのインスタンス１１１に関して使用管理判定を行うことが指示される。

【０２１７】

図６は、本発明の好ましい実施形態における装置（すなわち１０４）のタグテーブル２１０を示す。インストールされた各ソフトウエアのインスタンス１１１～１１４に対して、図５のステップ２５１を介して得られた各有効なタグＴＡＧ＿ＩＮＳＴ＿ＳＷ１２０は、タグテーブル２１０の“ＴＡＧＳ”のラベルをもつ第１欄に格納されている。タグテーブル２１０のＴＡＧＳ欄の中のタグは、ＴＡＧ＿ＩＮＳＴ＿ＳＷ１、ＴＡＧ＿ＩＮＳＴ＿ＳＷ２、ＴＡＧ＿ＩＮＳＴ＿ＳＷ３、ＴＡＧ＿ＩＮＳＴ＿ＳＷ４およびＵＮＴＡＧＧＥＤ＿ＳＷのラベルをもつ。詳述されるタグテーブル２１０の中の他の情報は、各タグに対してＵＳＡＧＥ　ＳＴＡＴＵＳリスト（第２欄）、ＡＣＴＩＯＮ　ＴＩＭＥ（第３欄）、ＲＵＮ　ＣＯＵＮＴ（第４欄）およびＵＳＥ　ＴＩＭＥ（第５欄）を含む。管理プログラム（ＳＰ）２０９は、各タグエントリー（すなわち各タグテーブル列）に対するタグテーブル情報を使用することにより、該当タグＴＡＧ＿ＩＮＳＴ＿ＳＷに付随するソフトウエアの各インスタンス１１１～１１４の使用の要求をどう処理するかを決める。

【０２１８】

簡単に説明すれば、タグテーブル２１０のＵＳＡＧＥ＿ＳＴＡＴＵＳ欄は、一般に管理プログラム２０９に対し、ソフトウエアのインスタンス１１１～１１４が、ユーザー２１３、または装置１０４～１０７に対して使用可能か否かを表示する。ソフトウエアの使用が許される時には、ステータス欄は“ＣＯＮＴＩＮＵＥＤ”、または“ＩＮＳＴＡＬＬＥＤ”を示すのに対し、使用が否認される時には、この状態は“ＧＣ＿ＤＩＳＡＢＬＥＤ”の語により示される。“ＲＥＭＯＶＥＤ”ステータス語が次に続く“ＩＮＳＴＡＬＬＥＤ”は、ソフトウエアのインスタンス１１１～１１４に対するタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎが、以前にはユーザー装置１０４にインストールされていたがもはやインストールされておらず、したがって使用可能ではないことを示す。ＡＣＴＩＯＮ　ＴＩＭＥ欄は、管理プログラム（ＳＰ）２０９（図２）により行われた最後のステータス判断（例えば、説明されるべき、最後の呼び出しおよびタグ確認手順）のタイムスタンプ（例えば日時）を示す。タグテーブル２１０のＲＵＮ　ＣＯＵＮＴ欄は、タグＴＡ

Ｇ＿ＩＮＳＴ＿ＳＷｎ（ただし、ｎはこの例では１から４の数字である）に付随するソフトウエアのインスタンス１１１～１１４がユーザー装置１０４～１０７に用いられた関数を示す。最後に、タグテーブル２１０におけるＵＳＥ　ＴＩＭＥ欄は、ＴＡＧ＿ＩＮＳＴ＿ＳＷｎに付随するソフトウエアのインスタンス１１１～１１４が装置と保護センターとの間の最後の呼び出し手順以来、または他の実施形態ではインストールされて以来経過した使用全時間を示す。

【０２１９】

各タグ（第１欄）に付随する各種の領域（すなわち列）は、この中で説明された各種の目的のために、この発明のシステムにより用いられる。タグは、付随の列の内容に基づいて特定のソフトウエアインスタンス１１１～１１４が適性に、または有効に使用されることができることを確かめるために調べなければならないタグテーブル２１０の列を特定するのに用いられる。選ばれた列の現在のＵＳＡＧＥ＿ＳＴＡＴＵＳ領域は、ソフトウエアインスタンス（すなわちこの列の１１１～１１４の１つ）の使用が許されるか否かを判定する。

【０２２０】

使用が許される時に説明されるように管理プログラム（ＳＰ）２０９は、使用されているインスタンス１１１～１１４に対する使用時間およびランカウントを追跡することができる。この情報は、ユーザー装置１０４～１０７の事象履歴を構成するために使用することが可能であり、ソフトウエアのインスタンス１１１～１１４のｐａｙ－ｐｅｒ－ｕｓｅ、またはｐａｙ－ｐｅｒ－ｖｉｅｗでの使用の追跡のような他の目的にも用いることができる。事象履歴は、すべての試みられた使用、完了した使用、使用時間および装置でのパワーアップのような他の事象のすべての時間的記録である。２つの装置により、それらがたとえ同じソフトウエアインスタンスおよび同じ識別子をもっていても同じ事象履歴をもつことは考えられない。

【０２２１】

ある実施形態において２つの装置は、同じソフトウエアインスタンスおよび同じタグ、または管理プログラム、または装置識別番号をもつことはない。しかし、ソフトウエアに対する狡猾な権利侵害者は、１つの装置のディスクイメージを

別のものに正確にコピーすることを試みることができ、この場合にはタグ、装置および管理プログラム識別子は、正確に複製されることがあり得る。本発明は、ある実施形態においてその識別子（例えばタグ１２０（図６の第１欄）、装置間のＳＰ　ＩＤ２０９－Ａ）に特定のプロセッサ、またはハードウエアシャーシを付随させる情報、例えばハードウエアプロセッサ識別番号（すなわち、例えばプロセッサの通し番号）を含めることを固有の識別子の少なくとも１つ（すなわちソフトウエアタグ１２０、または管理プログラム識別番号２０９－Ａの１つ）にとって可能にすることにより、このような侵害行為の回避を意図する。すなわち、侵害者が全ディスク情報を複製し、複製されたディスクを別の装置に移すことにより、本発明の使用管理保護をくぐり抜けることを試みる時、本発明はハードウエア装置識別機構を情報の中に組み入れ、タグの確認中（すなわち、説明されるべき呼び出し処理中）ハードウエア識別情報がそれにしたがってチェックされることができる。

【０２２２】

この実施形態は、同じタグ情報を用いることに努める２つの装置を追跡するために、保護センター１０３（図２）において保持される装置の使用統計値を用いる発明機構を補填すると理解されるべきである。すなわち、侵害者が合法的な装置１０４からのディスクを他の装置（すなわち１０７）にコピーする時には、この発明の構成によれば、装置の海賊版１０７の違法なユーザーにとって、この装置１０７を、合法的な装置１０４の使用を正確に複製する方法で使用することはほとんど不可能である。したがって、各装置１０４，１０７がタグの確認を行うために保護センター１０３（図２）に対して呼び出しを行う時に、保護センター１０３（図２）は、装置１０４，１０７の１つを、他の装置（すなわち１０４，１０７の他のもの）に関して不整合の使用または呼び出し統計値をもつとして検出する。したがって、各装置１０４，１０７が呼び出しを行った場合、装置１０４，１０７の１つは、不正のソフトウエアの使用を試みるように見える。この点で本発明のシステムは、継続メッセージ（後述される）に含まれる報復措置を実行することにより、一方または両方の装置、装置のソフトウエア、装置の使用、またはそれらの組み合わせの機能を停止することができる。違法または不法な使

用の正しい機関（例えば法務機関、ソフトウエアベンダー）への報告もまた本発明により行うことができる。

【０２２３】

ｐａｙ－ｐｅｒ－ｕｓｅ、またはｐａｙ－ｐｅｒ－ｖｉｅｗの例としてｐａｙ－ｐｅｒ－ｕｓｅソフトウエアのインスタンス１１１～１１４が用いられるたびに管理プログラム（ＳＰ）２０９は、そのインスタンス１１１～１１４に付随するタグＴＡＧ＿ＩＮＳＴ＿ＳＷに対し、タグテーブル２１０におけるＲＵＮ＿ＣＯＵＮＴ領域（第４欄）にこれを記録することができる。ＲＵＮ　ＣＯＵＮＴ情報は、後に請求の目的に用いることができる。

【０２２４】

またタグテーブル２１０に含まれているのは、この特定のユーザー装置１０４に対する特定のタグテーブル２１０を一意に識別するヘッダ領域ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥである。ヘッダＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥは、ｐｅｒ　ｕｓｅｒ２１３、またはｐｅｒ　ｕｓｅｒ　ｄｅｖｉｃｅ１０４ベースにおいて固有であることが可能である。タグテーブル２１０がｐｅｒ　ｕｓｅｒ２１３ベースで固有である時には、ユーザー装置１０４での各ユーザーアカウント（すなわちｌｏｇｉｎアカウント）は、そのユーザー２１３に対して独自のタグテーブル２１０をもつことができる。ｐｅｒ　ｕｓｅｒタグテーブル２１０は、そのユーザー２１３のみにより購入されているはずのソフトウエアのインスタンス１１１～１１４に対して、タグＴＡＧ＿ＩＮＳＴ＿ＳＷを使用されるために保持することができる。言い換えれば、唯１つのタグテーブル２１０が図示されているが、本発明はタグ使用および使用管理を多くのユーザー２１３において追跡することが可能であり、また各ユーザーは別個のタグテーブル２１０をもつことができる。

【０２２５】

ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥは、好ましくはこのタグテーブル２１０に対し固有の識別を示すＩＤ＿ＴＡＧ＿ＴＡＢＬＥ領域を含む。ＩＤ＿ＴＡＧ＿ＴＡＢＬＥ領域は、好ましくは管理プログラムの２０９ＩＤ（ＳＰ）２０９－Ａの識別を含む。さらにそれは、このタグテーブル２１０が付随するユーザー２１３

ＩＤ（ＵＳＥＲ）の識別ならびにユーザー装置１０４ＩＤ（ＤＥＶＩＣＥ）（例えば前述のように続き番号、またはｈｏｓｔ－ｉｄ）の識別およびオペレーティングシステム２０７ＩＤ（ＯＳ）の識別を含むことができる。

【０２２６】

ユーザー識別ＩＤ（ＵＳＥＲ）の例は、ユーザーネームおよび／またはパスワードの組み合わせであることができる。ユーザー装置ＩＤ（ＤＥＶＩＣＥ）の識別の例は、ホストネーム、ｈｏｓｔ　ｉｄ、ＩＰアドレス、続き番号、またはこのユーザー装置を、他のユーザー装置（例えば図１の１０４～１０７）と一意に識別することのできる他のハードウエアまたは装置についての特定の情報を含むことができる。

【０２２７】

ＩＤ（ＳＰ）２０９－Ａは、例えば装置１０４～１０７が高精度クロック（図４の２０５）に基づいて最初に通電される時点に関する情報からなることができる。異なった装置（すなわち１０４，１０５）からの２つのＩＤ（ＳＰ）’ｓ２０９－Ａは、高精度クロック２０５がマイクロセカンドの精度である時には等しくなるのはまれである。ＩＤ（ＳＰ）’ｓが等しくなることのリスクを低下させるには、ＩＤ（ＳＰ）２０９－Ａが、利用可能ならばハードウエア続き番号および利用可能ならば保護センター１０３（図２）からの番号を含むことも可能である。侵害者予備軍にとってディスクイメージをコピーすることは可能であるが、この場合には、２つの装置は同じＩＤ（ＳＰ）をもつかもしれない。上に簡単に触れたように、またさらに考察されるように、これは、呼び出し中保護センター１０３（図２）により捕捉されることができる。オペレーティングシステム２０７は、ＩＤ＿ＴＡＧ＿ＴＡＢＬＥに領域での識別に用いることができる続き番号、または同等の固有の識別情報をもつこともできる。

【０２２８】

ヘッダ領域ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥ（図６のタグテーブル２１０の上列）は、また“最後の保護センター継続メッセージ”領域ＬＡＳＴ＿ＧＣ＿ＣＭ、“最後の呼び出し時刻”領域ＬＡＳＴ＿ＣＡＬＬＵＰ＿ＴＩＭＥおよび“装置パワーアップの回数”領域ＮＵＭＢＥＲ＿ＤＥＶＩＣＥ＿ＰＯＷＥＲＵＰＳを

含む。さらにヘッダは、事象履歴を扱う二つの領域を含む：現在の事象履歴：ＨＡＳＨ（ＥＶＥＮＴ＿ＨＩＳＴＯＲＹ）および前回の呼び出し時点の事象履歴のハッシュ

ＨＡＳＨ（ＥＶＥＮＴ＿ＨＩＳＴＯＲＹ＿ＡＳ＿ＯＦ＿ＭＯＳＴ＿ＲＥＣＥＮＴ＿ＣＡＬＬＵＰ）。

【０２２９】

ヘッダのＬＡＳＴ＿ＧＣ＿ＣＭ領域（テーブル２１０の第１列）は、タグテーブル２１０更新情報の符号化を含む保護センター（ＧＣ）１０３（図２）からの偽造不能のメッセージである継続メッセージ値およびユーザー装置の管理プログラムＳＰに対するＧＣ１０３（図２）により定められた措置および報復措置を含む。タグテーブル２１０ヘッダにおけるＬＡＳＴ＿ＣＡＬＬＵＰ＿ＴＩＭＥは、ＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹにしたがっていつ次のＧＣ１０３（図２）への呼び出しが要求されるかを求めるために、管理プログラム２０９により、他のタグテーブルデータと組み合わせて使用される。ＮＵＭ＿ＤＥＶＩＣＥ＿ＰＯＷＥＲＵＰＳは、いつ呼び出しが必要であるかを定めるための方法の一部として使用される。

【０２３０】

事象履歴は、装置１０４～１０７の各ソフトウエアインスタンス１１１～１１４が実行される時、また場合によってはユーザー装置１０４～１０７に対する外部入力（すなわちユーザー装置２１３相互作用）が起きる時のような情報を含むことができる。事象履歴の目的は、その過去の挙動、または装置の使用に基づき装置１０４～１０７を識別することにある。これは、有用であると考えられる。なぜならば、管理プログラム識別番号２０９－Ａおよびタグ１２０のような静的情報は、１つの装置１０４～１０７から他の装置にコピーできるが、事象履歴に具現化された動的情報は、同じ静的情報をもつ装置１０４～１０７に対しても発散することが考えられるからである。事象履歴は大きいことがあるから、事象履歴のハッシュ関数値が、事象履歴自体に代わって保持される。好ましくは、２つの事象履歴ハッシュ関数値は、呼び出し手順中に処理を続けさせるために保有される。

【０２３１】

次に説明されるように好ましくは継続メッセージＣＭ（図２の２１２：図１３Ｂの４２３）は、タグテーブルヘッダのＬＡＳＴ＿ＧＣ＿ＣＭ領域にも格納される（図６のテーブル２１０の上列）。ＣＭ２１２は、ユーザー装置１０４による呼び出し手順中保護センター１０３（図２）により作られるメッセージであり、好ましくは、保護センター１０３（図２）により呼び出しを実行する装置１０４～１０７に安全に伝送される。継続メッセージＣＭ２１２は、ユーザー装置１０４に関する管理プログラム（ＳＰ）２０９がソフトウエアのいずれのインスタンス１１１～１１４が引き続き使用することを許されるか、または不正使用のために機能停止されるべきかを決めることが可能な情報を含み、また装置の管理プログラム２０９により実行すべき他の措置または報復措置を決定することもできる。

【０２３２】

ＬＡＳＴ＿ＣＡＬＬＵＰ＿ＴＩＭＥ領域は、発生した最後の呼び出し処理（説明あり）のタイムスタンプを含み、ＮＵＭ＿ＤＥＶＩＣＥ＿ＰＯＷＥＲＵＰＳ領域は、ユーザー装置１０４がパワーアップされた時点の数を含む。次に説明されるように、各ユーザー装置１０４における管理プログラム（ＳＰ）２０９は、ＮＵＭ＿ＤＥＶＩＣＥ＿ＰＯＷＥＲＵＰＳ、ＬＡＳＴ＿ＣＡＬＬＵＰ＿ＴＩＭＥおよびＬＡＳＴ＿ＧＣ＿ＣＭ継続メッセージのようなヘッダ情報を含むタグテーブル２１０の正確な情報を維持する（必ずしも作り出すことはない）ことに対して責任を負う。すなわち、継続メッセージ（ＣＭ）２１２（図２）は、保護センター１０３（図２）により作り出され、ユーザー装置１０４への管理プログラム（ＳＰ）２０９に安全に渡される。これを受け取ると管理プログラム（ＳＰ）２０９は、好ましくは継続メッセージ（ＣＭ）２１２（図２）をパースし、タグテーブル２１０を最新の使用管理情報により更新する（すなわちタグテーブル領域を更新）ことに責任を負う。

【０２３３】

ヘッダ領域ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥの中の情報は、一意的にタグテーブル２１０を識別することが可能であり、ユーザー装置１０４にインストール

されたソフトウエアの各インスタンス１１１～１１４に対する使用管理情報を更新するために使用することができる。この考え方では、各ユーザーまたは各ユーザーおよび／またはユーザー装置１０４の組み合わせに対するタグテーブル２１０は、他のユーザー２１３、または他のユーザー装置１０４、またはユーザー／ユーザー装置の組み合わせに対する他のタグテーブル２１０から、ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥを介して一意的に識別されることができる。

【０２３４】

ソフトウエアの新しいインスタンス１１１～１１４およびその付随のタグ１２０が図５のステップを介して入手され、インストールされ、使用される時に、そのタグＴＡＧ＿ＩＮＳＴ＿ＳＷに対するタグテーブル２１０エントリー（すなわちタグテーブル２１０の列）は、そのタグに付随するソフトウエアのインスタンス１１１～１１４がそのユーザー装置１０４に新たに追加され、またはインストールされることを示すためのＡＣＴＩＯＮコラム値を、ＩＮＳＴＡＬＬＥＤにセットされている。ＡＣＴＩＯＮ　ＴＩＭＥ値は空白にされるか、またはインストール時点を示す。ＲＵＮ　ＣＯＵＮＴおよびＵＳＥ　ＴＩＭＥコラム値はゼロ、または“０”にセットされ、または空白にされる。

【０２３５】

本発明の別の構成によれば、タグテーブル２１０に挿入するために作り出されたタグＴＡＧ＿ＩＮＳＴ＿ＳＷ（Ｃｏｌｕｍｍ１）を付随させていないソフトウエアインスタンス１１１～１１４に対して、使用管理を施すことができる。このようなインスタンス１１１～１１４は、ソフトウエアのタグをもたないインスタンス、またはタグなしのソフトウエアとも呼ばれる。タグなしのソフトウエアの例は、ユーザー２１３により作られたソフトウエアである。ユーザーにより作られたソフトウエアは、ソフトウエアプログラムもしくは歌を書きまたは創出するユーザー２１３の場合のように、合法的に作り出されることができる。ユーザーにより創出されるソフトウエアは、非合法的に作り出されることもあり、この場合には侵害ソフトウエアＩＮＦ＿ＳＷと呼ばれる。ユーザー装置１０４～１０７が合法的なタグなしのソフトウエアを使用することは望ましいことであり、本発明の使用管理はこのような使用を可能にする。しかし、同時に本発明の機構によ

れば本発明は、ユーザー装置１０４～１０７がタグありまたはタグなしの侵害ソフトウエアの使用を試みる時には、使用を検出し、阻止し、また必要ならばその装置に対して報復措置を定めることができる。

【０２３６】

侵害ソフトウエアＩＮＦ＿ＳＷは、例えば次のように作り出されることができるであろう。侵害者ベンダーは、本またはＣＤ－ＲＯＭのアプリケーションプログラムのような合法的特定のソフトウエアインスタンス１１１～１１４を用い、必要とされるタグ１２０の関連事項のすべてを、そのソフトウエアに対して含められたインストールプログラムから除去することにより、ソフトウエアインスタンスの海賊版を作り出すことができる。侵害者ベンダーは、次に変更されたソフトウエアのコピー（すなわち付随タグの引用をもはや必要としない）を別の名でタグなしのソフトウエアとして販売するのであろう。タグなしのソフトウエアの別の例は、ベンダーの本の別の言語への無許可の翻訳、またはアプリケーションプログラムの再コンパイルされたバージョンのような合法的なベンダーのソフトウエアＳＷの変造、または派生したバージョンとして侵害により作られた侵害ソフトウエアである。本発明のシステムは、ユーザー装置１０４～１０７におけるこのような不許可のソフトウエアに対し、使用を防止し、追跡し、防護する。

【０２３７】

前記を行うために本発明は、指紋と呼ばれるコンセプトを導入する。本質的に指紋は、そのインスタンスに対するソフトウエア（ＳＷ）の内容に対して固有の、ソフトウエアのインスタンスに付随する値を作り出す。ソフトウエアのインスタンスの違法に作り出されたコピーの指紋を入手することができる時には、本発明は同様に違法に作られたコピーを使用することの他のユーザー装置１０４～１０７による別の試みを検出するための方法を提供する。本発明によればソフトウエアの特定のピースに付随する指紋は、好ましくはユーザー２１３がユーザー装置１０４にタグなしのソフトウエアをインストールし、または使用することを試みる時である。

【０２３８】

図７は、ユーザー装置のタグなしのソフトウエアをインストールする処理を図

示する（この例ではユーザー装置１０４は考察の中で用いられる）。ステップ３３０においてユーザー装置２１３は、タグなしのソフトウエアのインスタンス（すなわち１１１～１１４のタグなしインスタンス）をユーザー装置１０４にインストールする（または作り出す）。タグなしのソフトウエアＵＮＴＡＧＧＥＤ＿ＳＷは、例えば単にバイナリーデータのストリングのように見え（ＳＴＲＩＮＧ〔０・・・Ｎ〕）、最初は付随のタグをもたない。ステップ３３１のタグなしのインスタンス１１１～１１４の使用が試みられると管理プログラム（ＳＰ）２０９は、このソフトウエアのインスタンスに対してタグテーブル２１０にはタグＴＡＧ＿ＩＮＳＴ＿ＳＷが存在しないことを検出し、したがって管理プログラム（ＳＰ）２０９は、指紋関数ＦＰを用いてタグなしのソフトウエアインスタンス１１１～１１４を指紋付けする。指紋関数は、例えばハッシュ関数であることが考えられる。

【０２３９】

ステップ３３１において各指紋Ｘｉは、好ましくはタグなしのソフトウエアの部分ＳＴＲＩＮＧ〔ｉ、ｉ＋ｋ－１〕において動作する指紋関数ＦＰにより作り出される値に等しい、ただし０＜＝ｉ＜＝ｍ－Ｋ＋１（定数Ｋに対して）。ｍ個のインデックスを選ぶことが可能である。言い換えれば指紋関数ＦＰは、タグなしのソフトウエアデータＳＴＲＩＮＧ〔０・・・Ｎ〕の選ばれたセグメント上で行われる、ただしＮはビット単位のタグなしのソフトウエアの全長である。好ましくは指紋関数ＦＰは、複数個の指紋（ｍ）を作り、そのそれぞれは他との間にオフセットを示す。ステップ３３２において管理プログラム（ＳＰ）２０９は、ユーザー装置１０４の指紋テーブル２１０が指紋Ｘｉ１からＸｉｍを格納する。

【０２４０】

前記に代わる実施形態においては指紋は、タグなしのソフトウエアの非連続部分に基づいて作られる。

【０２４１】

別の代わりの実施形態においては指紋は、ソフトウエアが用いられる時にソフトウエアの挙動に基づいて算定される。挙動の例は、ソフトウエアが行うシステムコールのシーケンスであることが可能である。例えば、ゲームソフトは、スク

リーンへの書き込みに特別のパターンをもつことができる。これらのパターンは、ソフトウエアのインスタンスの指紋に使用される。

【０２４２】

最後にステップ３２７において管理プログラム（ＳＰ）２０９は、ユーザー装置上のタグなしのソフトウエアのインスタンス１１１～１１４の存在を示すためのタグテーブル２１０のタグなしのタグエントリーＵＮＴＡＧＧＥＤ＿ＳＷを作り出す。タグテーブル２１０におけるＵＮＴＡＧＧＥＤ＿ＳＷタグは、指紋付けが行われたソフトウエアのタグなしのインスタンスにタグＵＮＴＡＧＧＥＤ＿ＳＷを一意的に付随させるために、ハッシュ関数または他の手段を用いることができる。前記の処理を用いることによりユーザー装置１０４にソフトウエアのタグなしのインスタンス１１１～１１４を使用し、またはインストールする試みは、そのタグなしのインスタンスが指紋付けされ、またＵＮＴＡＧＧＥＤ＿ＳＷタグがタグテーブル２１０の中に作り出される結果をもたらす。

【０２４３】

下記に説明されるように指紋テーブル１２６は、保護センター１０３（図２）が認めた侵害ソフトウエアＩＮＦ＿ＳＷの使用を検出するために保護センター１０３（図２）により使用される。この発明の指紋構成の使用の詳細は後述される。

【０２４４】

図８は、ユーザー２１３がソフトウエアのインスタンス（ＩＮＳＴ＿ＳＷ）１１１～１１４をユーザー装置１０４において使用することを試みる時にこの発明のシステム１０９により行われるハイレベルステップを示す。ステップ２７０においてはユーザー２１３は、ソフトウエアのインスタンス１１１～１１４を使用するためにユーザー装置１０４のユーザー入／出力機構２０４にインターフェースする。ステップ２７１においては管理プログラム（ＳＰ）２０９は、ソフトウエアのインスタンス１１１～１１４を使用させるためのコールを阻止する。この点で管理プログラム（ＳＰ）２０９は、要求されたタグテーブル２１０における“ＣＯＮＴＩＮＵＥＤ”ステータスを示すタグＴＡＧ＿ＩＮＳＴ＿ＳＷをもつことを確かめる。しかし、好ましい実施形態において個別のタグＴＡＧ＿ＩＮＳＴ

＿ＳＷｎをチェックする前に管理プログラムは、タグテーブル２１０自身が有効な、または更新された状態にあることを確かめる。有効な状態により意味されることは、タグテーブル２１０は、期限切れになっておらず、その内容を更新するために呼び出し手順を必要としていることである。したがってステップ２７２においては管理プログラム（ＳＰ）２０９は、保護センター１０３（図２）への呼び出しが現時点で必要であるか否かを確かめるために、タグテーブル２１０をアクセスする。

【０２４５】

前記に代わる実施形態において指紋がタグにおいて含められている時には、管理プログラムＳＰ２０９は、使用されているソフトウエアが同じ位置の指紋を用いることにより、このタグに正しく付随していることをチェックすることができる。

【０２４６】

呼び出し手順は、有効性を効果的に再確認し、タグテーブル２１０内での各タグＴＡＧ＿ＩＮＳＴ＿ＳＷｎの使用管理方針を実行するために、本発明のシステムにより定期的に行われる。呼び出し処理は、保護センター１０３（図２）とユーザー装置１０４との間で行われる。保護センター１０３（図２）に対して行われるべき呼び出しを行わせる引き金となる多くの事象の存在が考えられる。

【０２４７】

例えば、管理プログラム（ＳＰ）２０９によりステップ２７２において行われる呼び出しの決定は、タグテーブルヘッダＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥのＬＡＳＴ＿ＣＡＬＬ＿ＵＰ＿ＴＩＭＥ領域を調べることにより行うことができる。ＬＡＳＴ＿ＣＡＬＬ＿ＵＰ＿ＴＩＭＥにおけるタイムスタンプがある経過時間を越えている時には、保護センター１０３（図２）に対する呼び出しが必要であり、呼び出しの処理が行われるステップ２７３に移行することにより行われる。前記の代わりに要求される呼び出しのために満足されねばならない１群の原則、または条件を限定するタグテーブル２１０自身に対して呼び出し方針（ＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹ）が考えられる。

【０２４８】

他の実施形態においては、ソフトウエアの個々のインスタンス１１１～１１４に付随する呼び出し方針（ＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹ＿ＳＷ）の存在が考えられる。この場合にステップ２７２は、ソフトウエアコンテントＳＷ、またはステップ２７０におけるユーザー２１３により要求されたアクセスであったソフトウエアのインスタンス（ＩＮＳＴ＿ＳＷ）１１１～１１４に付随する呼び出し方針（ＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹ＿ＳＷ）のルール、またはテストを調べることができる。別の実施形態においてはユーザー装置１０４のユーザー２１３がソフトウエアのタグなしのインスタンスを使用することを試みる時には、ステップ２７２は呼び出しを必須条件とすることができる。別の実施形態においてはユーザー装置１０４のユーザー２１３が、初めはタグ付きソフトウエアを使用し、次にステップ２７２は、呼び出しを必須条件とすることができる。別の実施形態において継続的な呼び出し手順の間に許される最大間隔は、好ましくはユーザー装置１０４における経過時間、ソフトウエアのインスタンス１１１～１１４の使用の回数と使用時間、装置１０４のパワーアップの回数および／または装置１０４の時間または使用に関する他の手段の組み合わせにより決まる。

【０２４９】

呼び出しの処理は後に詳細に考察される。しかし、本質的に呼び出しの処理中は、ユーザー装置１０４の中の管理プログラム（ＳＰ）２０９が、タグテーブル２１０および指紋テーブル１２６のコピーを保護センター１０３（図２）に安全に引き渡す。確認後保護センター１０３（図２）は、タグテーブル２１０の各タグＴＡＧ＿ＩＮＳＴ＿ＳＷｎを損なわれたタグのリストと比較する。保護センター１０３（図２）は、ある方法で無効、または損なわれたタグを検出することができる。

【０２５０】

各タグに付随する使用管理方針ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）は、タグ１２０（およびしたがってタグに付随するソフトウエアのインスタンス）が使用管理方針ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）に基づいて使用されていることを確かめるために保護センター１０３（図２）においてチェックすることもできる。方針は、全ユーザー装置１０４～１０７、またはｐｅｒ　ｕｓｅｒ２

１３、またはｐｅｒ　ｔａｇ１２０ベースであることができる。またタグなしのソフトウエアに対しては、指紋テーブル１２６は侵害ソフトウエアＩＮＦ＿ＳＷの使用を検出するために保護センター１０３（図２）の指紋データ構造体（後に説明あり）に対して比較することができる。タグテーブル２１０および指紋テーブル１２６の分析が完了した後、保護センター１０３（図２）は、継続メッセージ（ＳＭ）２１２（図２）を作りユーザー装置１０４に送り返す。

【０２５１】

前記に代わる実施形態においてタグ付きのソフトウエアは、また指紋によってチェックすることができる。この実施形態は、侵害者ベンダーが、知的所有物または合法的なベンダー（すなわち１０１）の他の権利を侵害する特定のソフトウエアのインスタンスを、タグ付きすなわちタグサーバー１０２から入手した合法的なタグを添えられたソフトウエアとして配布することを防止する。この実施形態においてはユーザー装置１０４～１０７の管理プログラム２０９は、タグ付きのソフトウエアインスタンス１１１～１１４においても指紋処理を実行し、算定された指紋をその指紋テーブル１２６に格納する。呼び出し手順中にユーザー装置１０４～１０７に用いられるタグ付きのソフトウエアインスタンス１１１～１１４から得られる指紋もまた侵害ソフトウエアの使用を検出するために保護センター１０３（図２）に送られる。

【０２５２】

継続メッセージ（ＣＭ）２１２（図２）は、ユーザー装置（例えば１０４）のソフトウエアのインスタンス１１１～１１４の動作、または装置１０４自身の動作に影響を及ぼすことのある各種の情報を含む。例えば、保護センター１０３（図２）がユーザー装置１０４に対しタグテーブル２１０における無効のタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎを検出すると、そのユーザー装置１１０４に戻された継続メッセージ（ＣＭ）２１２は、ユーザー装置１０４に対し特定の時間にわたり、または無制限に機能を停止させることができる。あるいは前記に代わり継続メッセージ（ＣＭ）２１２は、ユーザー装置１０４が無効タグ１２０に付随するソフトウエアの特定のインスタンス（ＩＮＳＴ＿ＳＷ）を使用するのを無効にすることができる。

【０２５３】

ユーザー装置１０４において実行される措置は、継続メッセージ（ＣＭ）２１２のＡＣＴＩＯＮＳ部分において限定され、後に詳述される。継続メッセージ２１２は、またタグテーブル２１０における情報を更新するためにユーザー装置１０４における管理プログラム（ＳＰ）２０９によって使用される。例えば、そのタグテーブル２１０のＡＣＴＩＯＮ　ＴＩＭＥコラムは、最新の継続メッセージ（ＣＭ）２１２のタイムスタンプにより更新されることができるので、各タグＴＡＧ＿ＩＮＳＴ＿ＳＷｎが保護センター１０３（図２）により最近チェックされた時点を示すことができる。

【０２５４】

図８の処理の記述を続ける際にステップ２７３における呼び出し処理が完了した後タグテーブル２１０は、ステップ２７７におけるユーザー装置１０４において更新され（すなわち継続メッセージ２１２を介して）、処理はステップ２７２に戻る。ユーザー装置がこの時点で保護センター１０３（図２）への呼び出しが不必要と認めた時には、処理はステップ２７４に進み、ステップ２７３においてユーザー２１３により使用が要求されたソフトウエアの特定のインスタンス１１１～１１４の使用状況が求められる。

【０２５５】

ステップ２７４においてユーザー装置１０４の管理プログラム（ＳＰ）２０９は、要求されたソフトウエアのインスタンス１１１～１１４が付随するタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎに対するタグテーブル２１０におけるＵＳＡＧＥ　ＳＴＡＴＵＳコラムを重点的に調べる。ＵＳＡＱＥ　ＳＴＡＴＵＳコラムが“ＣＯＮＴＩＮＵＥＤ”を示す時には、管理プログラム（ＳＰ）２０９は、オペレーティングシステム２０７のカーネル２０８に信号を送ることにより、ステップ２７５の要求されたソフトウエアのインスタンス１１１～１１４の使用を許す。要求されたソフトウエアのインスタンス１１１～１１４に付随するタグ（ＴＡＢ＿ＩＮＳＴ＿ＳＷｎ）に対するタグテーブル２１０におけるＵＳＡＧＥ　ＳＴＡＴＵＳコラムが“ＧＣ＿ＤＩＳＡＢＬＥＤ”、または“ＲＥＭＯＶＥＤ”を示す時には管理プログラム２０９は、ステップ２７６でのソフトウエアのインスタンス１１１

～１１４の使用を否認する。

【０２５６】

要求されたソフトウエアのインスタンス１１１～１１４に使用が許されると管理プログラム（ＳＰ）２０９は、要求されたソフトウエアのインスタンス１１１～１１４が付随するタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎに対するＲＵＮ　ＣＯＵＮＴコラムにおける値を１つだけ増やす。管理プログラム（ＳＰ）２０９は、要求されたソフトウエアのインスタンス１１１～１１４が使用されている時間を追跡し、これに基づいてタグに対してＵＳＥ　ＴＩＭＥコラムを更新する。

【０２５７】

図９は、保護センター１０３（図２）の構造の好ましい実施形態を図示する。保護センター１０３（図２）は、プロセッサ３０１、メモリー３０２、相互接続機構３０３、クロック３０４および保護センター承認データベース３００を結合するバスを含む。保護センター１０３（図２）は、好ましくは１回に複数の処理のための多くの操作を行うことのできるマルチプロセッササーバーのようなハイパワードコンピューターシステムである。相互接続機構３０３は、例えば保護センター１０３（図２）がコミュニケーションネットワーク１００を介して同時に多くのユーザー装置１０４と通信することを可能にするモデムバンク、または１つ以上の高帯域幅ネットワーク接続である。

【０２５８】

保護センター１０３（図２）の承認データベース（ＧＣＤＢ）３００は、好ましくは広汎な量の情報を格納する能力もつ大きいデータベースサブシステム、またはディスク、またはＲＡＩＤアレーである。この実施形態においてＧＣＤＢは、タグ付きのソフトウエアのインスタンスに対するデータおよび指紋データ構造体１３７に対するデータを保持するタグ付きのソフトウエアデータベース１３８（図９）を含む。タグ付きのソフトウエアデータベース（図９）は、各ユーザー装置１０４のソフトウエアの各タグ付きインスタンスに対する呼び出し記録（図１０の３２０，３２１）を含む。これらのデータベース１３７および１３８（図９）のそれぞれの内容と使用は詳述される。

【０２５９】

保護センター１０３（図２）の動作中メモリ３０２は、プロセッサー３０１と関連してこの中に記された保護センター機能を実行する確認プログラム（ＶＲＰ）３１５を格納するのに用いられる。メモリ３０２は、またはタグの確認および上に簡単に説明された呼び出し手順中のタグ確認および使用管理決定のために、保護センター１０３（図２）に移されるユーザー装置タグテーブル２１０および指紋１２６に格納する。

【０２６０】

図１０は、タグ付きのソフトウエア（例えば１１１～１１４）各インスタンスに対し保護センター１０３（図２）でタグ付きのソフトウエアデータベース１３８（図９）に維持されるデータ構造体３２０，３２１を示す。タグデータ構造体３２０は、ソフトウエアの各インスタンス１１１～１１４に対するタグ１２０が作られた時に、タグサーバー１０２から保護センター１０３（図２）に最初に送られる。好ましくはタグサーバー１０２から保護センター１０３（図２）にタグ１２０が与えられる方法は、コミュニケーションネットワーク１００を通じ電子的で安全な配布によるものである。前記に代わり、ソフトウエアベンダー１０１は、ユーザー装置１０４～１０７に配布されるソフトウエアの各インスタンス１１１～１１４に対するタグ情報を常に知られていることを保障することの責任を負うことができる。

【０２６１】

タグデータ構造体３２０は、ユーザー装置１０４に用いられるソフトウエアの各インスタンスに対するタグ付きのソフトウエアデータベース１３８（図９）にある。図示されるように各タグデータ構造体３２０は、各種の領域を含む。これらの領域は、ソフトウエアのそのインスタンスに対するタグＴＡＧ＿ＩＮＳＴ＿ＳＷ、そのソフトウエアに対する使用管理方針ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）およびソフトウエアのそのインスタンスに対する１つ以上の呼び出し記録ＣＡＬＬ＿ＵＰ＿ＲＥＣＯＲＤｎ３２１に対する関連事項のリストを含む。

【０２６２】

ソフトウエアのインスタンス１１１～１１４に対するタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎに付随する方針ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）は、ソフトウエ

アベンダー１０１、または別の組織により定められ、使用権、またはタグに付随するソフトウエアのインスタンスに対するｐａｙ－ｐｅｒ－ｕｓｅアクセス制限の防護に関する規制と方針を規定する。例えばソフトウエアの特定のインスタンス１１１～１１４に付随するタグデータ構造体３２０に対しては、ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）データは、ソフトウエアのインスタンスを使用するごとにユーザー装置１０４が定められた料金を支払わねばならないことを内容とする規制を含むことができる。

【０２６３】

呼び出し処理（後述される）の間、保護センター１０３（図２）がユーザー装置１０４からタグテーブル２１０を受け取る時に、そのユーザー装置１０４によりソフトウエアの特定のインスタンス１１１～１１４が使用された回数は、タグテーブル２１０のソフトウエアのそのインスタンスに対するタグＴＡＧ＿ＩＮＳＴ＿ＳＷに付随するタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎのＲＵＮ ＣＯＵＮＴコラムから求めることができる。保護センター１０３（図２）は、次にタグ付きソフトウエアデータベース１３８（図９）のそのタグＴＡＧ＿ＩＳＮＴ＿ＳＷｎに付随するタグデータ構造体３２０に対する方針ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）に依存することができる。保護センター１０３（図２）は、タグテーブル２１０の中のＲＵＮ　ＣＯＵＮＴ領域により示されている使用回数が前の呼び出し処理から得られた前の数よりも多いか否かを調べることをできる。数が多ければ、保護センター１０３（図２）は、ユーザー装置１０４のオーナーまたはユーザー２１３に送られるべき請求用のこの情報を記録することができる。

【０２６４】

他の使用管理方針ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）は、保護センター１０３（図２）がソフトウエアの特定のインスタンス１１１～１１４に対する特定の数の使用のみを可能にするように規定されることができる。使用回数を上回ると保護センター１０３（図２）は、ソフトウエアの前記のインスタンスにタグの付随したユーザー装置のタグテーブル２１０に付随するＵＳＡＧＥ　ＳＴＡＴＵＳ領域を値“ＧＣ＿ＤＩＳＡＢＬＥＤ”に送られることができる。タグテーブル２１０の分析後、そのユーザー装置１０４に保護センター１０３（図２）に送

られる継続メッセージ（ＣＭ）２１２に適切な情報を記載することにより、ユーザー装置１０４において変更を行うことができる。ユーザー装置１０４が機能を停止されているタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎ（すなわち図６のタグテーブル２１０のＴＡＧ＿ＩＮＳＴ＿ＳＷ３）に付随するソフトウエアのインスタンス１１１～１１４を使用することを試みる時には、図７において上に説明されているように使用は否認される。

【０２６５】

保護センター１０３（図２）の中のタグ付きのソフトウエアデータベース１３８（図９）における各タグデータ構造体３２０は、図１０に示された呼び出し記録ＣＡＬＬ＿ＵＰ＿ＲＥＣＯＲＤｎ３２１への引用回数を含む。呼び出し記録ＣＡＬＬ＿ＵＰ＿ＲＥＣＯＲＤｎ３２１は、呼び出しタイムＣＡＬＬ＿ＵＰ＿ＴＩＭＥ、コールするユーザー装置１０４のタグテーブル２１０からのヘッダ領域ＨＥＡＤＥＲ ＴＡＧ＿ＴＡＢＬＥ、タグテーブル２１０ＨＡＳＨ（ＴＡＧ＿ＴＡＢＬＥ）のハッシュ関数値、およびＡＣＴＩＯＮ領域を含む。したがって送られたタグの数に関係なく呼び出しごとに１つのＣＡＬＬ＿ＵＰ　ＲＥＣＯＲＤが生じる。

【０２６６】

ＣＡＬＬ＿ＵＰ＿ＴＩＭＥ領域が現在のＣＡＬＬ＿ＵＰ＿ＲＥＣＯＲＤｎに対する呼び出しのタイムスタンプを示す。ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥは、呼び出し手順ｎ中のコールするユーザー装置１０４から受け取られるこのタグデータ構造体３２０に対するＴＡＧ＿ＩＮＳＴ＿ＳＷｎを含むタグテーブル２１０のタグテーブルヘッダを含む。ＨＡＳＨ（ＴＡＧ＿ＴＡＢＬＥ）領域は、タグテーブル構造体３２０に付随するタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎを含んでいたタグテーブル２１０の中のデータのすべてについて算定された実現不能なハッシュ関数値を含む。最顎にＡＣＴＩＯＮＳ領域は、タグデータ構造体３２０に対してタグＴＡＧ＿ＩＮＳＴ＿ＳＷに付随するソフトウエアのインスタンス１１１～１１４に対して実行されるべき呼び出し手順ｎ中に保護センターにより定められた措置をリストする。ソフトウエアの各インスタンス１１１～１１４に対するタグデータ構造体３２０を用いる時に保護センター１０３（図２）は、ユーザー装置１

０４を介して用いられるソフトウエアのインスタンス１１１～１１４に対する使用管理機構に関連する詳細な情報を維持することができる。

【０２６７】

図１１は、保護センター１０３（図２）の中に維持されている指紋データ構造体１３７を作る結果となる処理ステップを示す。前記の、図７に関して説明されたように指紋は、タグなしのソフトウエア、および場合によってタグ付きソフトウエアもまた最初にユーザー装置１０４に用いられる時に、各ユーザー装置１０４の中の指紋テーブル１２６に格納される。本発明によればソフトウエア構成は、ベンダーソフトウエアをコピーし、タグの確認を要求するソフトウエアの部分を取り外し、または合法的なソフトウエアの派生体を作り配布することにより、合法的なベンダーの権利を侵害することが考えられる。このように作られたソフトウエアは、侵害されたソフトウエアＩＮＦ＿ＳＷと称される。保護センター１０３（図２）の中に作り出された指紋データ構造体１３７は、権利侵害のソフトウエアのインスタンスＩＮＦ＿ＳＷについて算定された指紋を含む。

【０２６８】

ステップ３４０の図１１においてソフトウエアベンダー１０１は、権利侵害のソフトウエアのインスタンスの存在を検出する。ステップ３４１においてソフトウエアベンダー１０１は、権利侵害のソフトウエアのインスタンスＩＮＦ＿ＳＷのコピーを保護センター１０３（図２）に提出する。侵害ソフトウエアは、ＳＴＲＩＮＧ＿ＩＮＦ〔０・・・Ｎ〕と見えるバイナリ数字（ビット）のストリングであるに過ぎない。ステップ３４２においては保護センターは、ユーザー装置１０４のそれぞれについて管理プログラム（ＳＰ）２０９が指紋を算定するために用いるのと同じ指紋公式ＦＲを用い、権利侵害のソフトウエアのインスタンスにおける指紋Ｙｉの収集物を算定する。すなわち一連の指紋Ｙｉは、下記のように計算される。

【０２６９】

Ｙｉ＝ＦＲ（ＳＴＲＩＮＧ＿ＩＮＦ〔ｉ、ｉ＋ｋ－１〕）

【０２７０】

ただし、０＜＝ｉ＜＝ｎ－ｋ＋１、ｎ－ｋは、算定する指紋の数である。次に

ステップ３４３において保護センター１０３（図２）は、算定された指紋Ｙ１，．．．Ｙｎ－ｋ＋１のそれぞれをＧＣＤＢ３００の中の指紋データ構造体１３７に使用する。前記に代わる実施形態において指紋は、ＳＴＲＩＮＧ＿ＩＮＦのノンコンセクティブシーケンスにおいて算定され、このシーケンスはＩＮＦ＿ＳＷに対して一意的、またはほぼ一意的である。

【０２７１】

指紋処理は、保護センター１０３（図２）において完了し、侵害ソフトウエアＩＮＦ＿ＳＷは破棄されるか、または他のコミュニケーションネットワーク１００のような他の場所での他の保護センター１０３において利用することができる。

【０２７２】

この時点でユーザー装置１０４に関する管理プログラム（ＳＰ）２０９が、タグのない（およびおそらく権利侵害する）ソフトウエアのインスタンスを使用することの要求を検出すると、管理プログラム（ＳＰ）２０９は、ＵＮＴＡＧＧＥＤ＿ＳＷの指紋を記録する。後にＳＰ２０９がタグテーブル２１０および指紋テーブル１２６を保護センター１０３（図２）に移すための呼び出し手順を実行する時には、記録されたＵＮＴＡＧＧＥＤ＿ＳＷの指紋が送られる。ある実施形態においてはタグなしのインスタンスを使用するためのユーザー装置１０４～１０７におけるアクセス要求は、呼び出しを発生させることがある。一般位置の指紋を用いることにより指紋テーブル１２６の指紋は、保護センター１０３（図２）の指紋データ構造体１３７における指紋と比較することができる。ソフトウエアインスタンスＵＮＴＡＧＧＥＤ＿ＳＷが保護センター１０３（図２）により感知され、それ自体に指紋付けを行った権利侵害のソフトウエアインスタンスＩＮＦ＿ＳＷのコピーである時には、このことは検出され、報復措置がユーザー装置１０４において継続メッセージ２１２の返却により行うことができる。別の実施形態においてはユーザー装置１０４のＵＮＴＡＧＧＥＤ＿ＳＷのシステムコールの挙動（すなわちシステムコールのシーケンス）は、保護センター１０３（図２）のＩＮＦ＿ＳＷについて予測されるシステムコール挙動と比較される。他の実施形態において最後の２パラグラフに詳述されたステップは、タグ付きのソフトウ

エアの使用に対するユーザー装置に関する要求の場合にも適用される。

【０２７３】

この発明の指紋構成とは別に、次に説明される呼び出し手順中保護センター１０３（図２）の確認プロズラム３１５は、タグテーブル２１０の情報を使用管理決定を行うためにタグソフトウエアデータベース１３８（図９）の情報と比較する。

【０２７４】

図１２は、本発明の好ましい実施形態での呼び出し手順を実行するためにユーザー装置１０４において実行される管理プログラム（ＳＰ）２０９により行われるステップを図示する。図１２のステップは、図８のステップ２７３の中で行われる。

【０２７５】

図１２におけるステップ３７０において管理プログラム（ＳＰ）２０９は、保護センター１０３（図２）を呼び出す。呼び出しとは、ユーザー装置１０４の管理プログラム（ＳＰ）２０９が、保護センター１０３（図２）にコミュニケーションネットワーク１００を介して接続され、またはメッセージを交換することを意味する。好ましい実施形態においては管理プログラム（ＳＰ）２０９は、ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥを保護センター１０３（図２）に送る。保護センター１０３（図２）は、装置のＩＤ＿ＴＡＧ＿ＴＡＢＬＥからなる前の継続メッセージ、最後の呼び出しの時間ＬＡＳＴ＿ＣＡＬＬＵＰ＿ＴＩＭＥが、この同じＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥをもつ最近のＣＡＬＬ＿ＵＰ記録のＣＡＬＬＵＰ＿ＴＩＭＥに等しくない限り、呼び出しエラーを生じる。この実施形態の利点は、たとえ数台の装置１０４～１０７が同じＩＤ＿ＴＡＧ＿ＴＡＢＬＥ（図６のタグテーブルの列１）および同じタグ２１０（普通侵害のために生じる）をもっていても、これらの同じ装置は同じ継続メッセージを受け取っても下記の理由で正しく受け入れることはなく、したがって唯１つの装置（すなわち１０４～１０７の１つ）が特定のＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥを送る。

【０２７６】

ユーザー装置１０４～１０７におけるソフトウエアのインスタンス１１１～１

１４をユーザーが使用することを試みる場合には、上に説明された通り、ＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹ、またはＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）にしたがって呼び出しが行われる。すなわち、ユーザー装置１０４のＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹによる次の呼び出しの前に時間が許されるか、またはそのインスタンスに対するソフトウエア（ＳＷ）のＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）が経過したソフトウエアのインスタンス１１１～１１４の使用をユーザー２１３が試みる時には、その装置１０４～１０７の管理プログラム２０９がステップ３７０を開示する。別の実施形態においてＳＰ２０９は、ソフトウエアのインスタンス１１１～１１４の使用が要求されているか否かには関係なく、時間の経過する前の選ばれた時点に呼び出し手順を実行する。ＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹは、ユーザー装置１０４の管理プログラム２０９の中に保持されることができる。さらに使用の要求とは関係なく実行される管理プログラム２０９の部分が、呼び出しを行う時点であることを求めることにより呼び出しが行われることが可能である。例えばユーザー装置１０４～１０７のある回数のＢＯＯＴＵＰＳ（パワーアップ）が行われた結果、またはタグなしのソフトウエアの最初の使用の結果起きることが考えられる。

【０２７７】

ステップ３７１の保護センター１０３（図２）に対する呼び出しが失敗すると、処理は、ユーザー装置１０４の管理プログラム（ＳＰ）により報復措置の行われることのあるステップ３７６に進む。好ましい実施形態において管理プログラム（ＳＰ）２０９は、新たな呼び出しを行い、報復措置を始める前に数回試みる。報復措置がステップ３７６において必要である場合には、報復措置は、単にユーザー２１３に要求されたソフトウエアのインスタンス１１１～１１４が、通信のエラーにより一時的にアクセス不能であることを通告するにとどめることが可能である。

【０２７８】

呼び出しが成功し保護センター１０３（図２）にユーザー装置１０４から接続が行われると、３７２において管理プログラム（ＳＰ）２０９は、好ましくはユーザー装置１０４から保護センター１０３（図２）にタグテーブル２１０を安全

に送るか、または送信する。代案の実施形態においては管理プログラム（ＳＰ）２０９は、指紋テーブル１２６を保護センター１０３（図２）にも送る。すなわち、本発明の指紋構成は、ユーザーにより作られ、またはユーザーにより変造された侵害ソフトウエアを検出するために実施形態に使用され、または使用されないことがある。

【０２７９】

ステップ３７２が完了した後、管理プログラム（ＳＰ）２０９は、継続メッセージ（ＣＭ）２１２が保護センター１０３（図２）との間にやりとりの行われるまでは待ちの状態に入る。前記の代わりに管理プログラムＳＰ２０９は、ステップ３７２が完了した後にスリープ状態に入り、オペレーティングシステム（ＯＳ）２０７から中断された後に再び走行する。前記に代わる実施形態において管理プログラムＳＰは、ユーザーからの処理要求に続く。保護センター１０３（図２）呼び出し処理は、図１３Ａおよび１３Ｂに関して後述される。保護センター１０３（図２）が呼び出し手段処理を終えると、継続メッセージ（ＣＭ）２１２がユーザー装置１０４に送られる。

【０２８０】

ステップ３７３においては、管理プログラム（ＳＰ）２０９は、ユーザー装置１０４の呼び出し方針ＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹに規定される継続メッセージ２１２の戻りをチェックする。呼び出し方針ＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹの中の継続メッセージ（ＣＭ）２１２に対するチェックの例として、ステップ３７３は、継続メッセージ（ＣＭ）２１２を受け取る前にある経過時間を上回っていないことを確かめることができる。継続メッセージ２１２の受け取り前に著しく時間が経過している場合には、呼び出し方針は背反されることがある。

【０２８１】

継続メッセージ２１２のデジタル署名を確認することのできるような呼び出しの背反が起きるか否かを調べるために他のファクターを用いることができる。呼び出し背反を決める別のファクタは、継続メッセージ２１２のＨＡＳＨ（ＥＶＥＮＴ＿ＨＩＳＴＯＲＹ）領域が最後の呼び出しの時点でユーザー装置１０４に記録された事象履歴のハッシュ、ＨＡＳＨ（ＥＶＥＮＴ＿ＨＩＳＴＯＲＹ＿ＡＳ＿

ＯＦ＿ＭＯＳＴ＿ＲＥＣＥＮＴ＿ＣＡＬＬＵＰ）とは同じでないことである。同じ構成およびＩＤ＿ＴＡＧ＿ＴＡＢＬＥをもつ２つの装置が侵害行為の結果存在するが、１つのみが呼び出しを行う場合には前記は起こり得る。事象履歴のために装置１０４～１０７の１つのみが継続メッセージ２１２を受け取る。他の装置は、自己の呼び出しを行うだけであり、このことが呼び出しのエラーを招く。なぜならば、ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥ（図６のテーブル２１０の第１列）は、ＩＤ＿ＴＡＧ＿ＴＡＢＬＥで合致するか、前記の理由で呼び出し時点で合致できないからである。

【０２８２】

ＣＡＬｌ＿ＵＰ＿ＰＯＬＩＣＹがステップ３７３において背反される時には、処理はステップ３７６に進み、また報復措置がユーザー装置１０４において行われることができる。この場合には、報復措置は、呼び出しが進むことができず、また要求されたソフトウエアのインスタンス１１１～１１４が一時的にアクセスを否認され、または機能を停止されねばならないことをユーザー２１３に通告することを含むことができる。前記に代わりユーザー装置１０４は、ある時間機能を停止されることができる。

【０２８３】

ステップ３７３が継続メッセージ（ＣＭ）２１２が受け取られ、ステップ３７４においてＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹに規定された限界内にあるために受け入れられることを認めると、継続メッセージ（ＣＭ）２１２が管理プログラム（ＳＰ）２０９に引渡される。次にステップ３７５において管理プログラム（ＳＰ）２０９が継続メッセージ２１２を、デジタル鍵署名技術を介して確認し、ユーザー装置１０４のタグテーブル２１０における各タグＴＡＧ＿ＩＮＳＴ＿ＳＷｎに対する継続メッセージ２１２における各措置を実行する。すなわち、管理プログラム（ＳＰ）２０９は、タグテーブル２１０の各タグＴＡＧ＿ＩＮＳＴ＿ＳＷｎに対するＵＳＡＧＥ　ＳＴＡＴＵＳおよびＡＣＴＩＯＮ　ＴＩＭＥ欄を更新する。この方法で本発明のシステム１０９は、ユーザー装置１０４が定期的にタグテーブル更新２１０を保護センター１０３（図２）から得ることが可能になる。

【０２８４】

管理プログラム（ＳＰ）２０９がユーザー２１３とユーザー装置１０４上のインストールされたソフトウエアのインスタンス１１１～１１４との間のインターフェースとして用いられるから、管理プログラム２０９は、好ましくはユーザー装置１０４の中に記載された使用管理機構を実行する。ソフトウエアのインスタンス１１１～１１４に対するタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎが呼び出し処理中にしか変更できない“ＣＯＮＴＩＮＵＥＤ”使用ステータス状態であることを要求することにより、使用管理は究極的に１つ以上の保護センター１０３（図２）により管理される。保護センター１０３（図２）は、ユーザー装置１０４に対するタグテーブル２１０におけるタグが、タグおよび指紋のために規定された方針通りに“ＣＯＮＴＩＮＵＥＤ”または“ＧＣ＿ＤＩＳＡＢＬＥＤ”状態になければならないか否かを決定することの責任を負う。

【０２８５】

図１３Ａおよび１３Ｂは、本発明の好ましい実施形態による呼び出し処理中に保護センター１０３（図２）の確認プログラム（ＶＲＰ）３１５により行われるステップを示す、１つの連続フローチャートを示す。保護センター１０３（図２）は、ユーザー装置１０４（すなわち、管理プログラム２０９）が最初の呼び出し処理接続、または図１２のステップ３０７の保護センター１０３（図２）との接触を行う時には、呼び出し手順を知らされる。これに応じて図１３Ａのステップ４１０では、確認保護センター１０３（図２）がタグテーブル２０１を受け取る。保護センター１０３（図２）は、またインストールされるがタグテーブル２１０の中のタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎにより、タグを施されていないソフトウエアがユーザー装置１０４にある時には、ユーザー装置１０４から指紋テーブル１２６を受け取る。この場合にも本発明の指紋構成は選択的であるが、本発明の好ましい実施形態には設けられている、なぜならば、それらは侵害ソフトウエアの検出を可能にするからである。

【０２８６】

前記に代わる実施形態においては保護センター１０３（図２）は、タグテーブル２１０のみの一部、例えばＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥおよびタグテーブル２１０の中のタグ（コラム１）の一部のみを受け取る。受け取られたタグ１

２０は、保護センター１０３（図２）が要求するか、または無作為に選ばれるか、またはその時点でのソフトウエアのインスタンスの使用のためにユーザー装置が必要とする唯１つのタグ１２０であることが可能である。別の可能性は、タグ１２０がｐａｙ－ｐｅｒ－ｕｓｅであるか、または一定の使用数をもつソフトウエアのインスタンスに相当することである。この代案の利点は、それが通信コストおよび処理コストをともに引き下げることである。

【０２８７】

別の代案実施形態においては、保護センター１０３（図２）がＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥ（図６のタグテーブル２１０の上列）のみを受け取る。この実施形態は、保護センター呼び出しを割安にし、各ＴＡＧ＿ＩＮＳＴ＿ＳＷが後述のようにＩＤ＿ＴＡＧ＿ＴＡＢＬＥ欄を含む時に充分に機能することができる。次にステップ４１１の図１３Ａに関する呼び出し処理の記述に戻る時、保護センター１０３（図２）は、ユーザー装置１０４に付随する呼び出し方針ＣＡＬＬ＿ＵＰＰＯＬＩＣＹにしたがっていることを確かめるためにチェックする。ユーザー装置１０４～１０７に対する呼び出し方針ＣＡＬＬ＿ＵＰ＿ＰＯＬＹＣＹ（Ｓ）は、好ましくは保護センター１０３（図２）において維持され、および／またはソフトウエアベンダー１０１、またはユーザー装置メーカー（図示されず）から必要に応じてユーザー装置１０４がそのタグテーブル２１０を確認し、更新しなければならないかを求める方法を、保護センター１０３（図２）にインストラクトするために提供されることができる。

【０２８８】

ステップ４１１は、例えばＩＤ＿ＴＡＧ＿ＴＡＢＬＥ領域に含まれるタグテーブル２１０の固有の識別のようなＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥ情報領域を用いて行うことができる。呼び出しがＣＡＬＬ＿ＵＰ＿ＰＯＬＩＣＹにしたがっていない時には、ステップ４１６は、継続メッセージ（ＣＭ）２１２が保護センター１０３（図２）からユーザー装置１０４に戻される時に管理プログラム（ＳＰ）２０９により実行されるための特別の報復措置を作る。

【０２８９】

ステップ４１６および４１１の両方からステップ４１２に処理が進み、この点

で確認プログラム３１５は、タグテーブル２１０の署名され、および／または署名されていないタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎを確認する。ステップ４１２において行われる確認は、タグテーブル２１０の署名されているタグＴＡＧ＿ＩＮＳＴ＿ＳＷに対するデジタル署名確認であることができる。署名されていないタグに対してＨＡＳＨ＿ＩＮＳＴ＿ＳＷ値は、タグＴＡＧ＿ＩＮＳＴ＿ＳＷの中の秘密番号ＮＵＭ＿ＩＮＳＴ＿ＳＷがそのタグに対するＨＡＳＨ＿ＩＮＳＴ＿ＳＷに一致することをチェックするために、用いることができる。これは可能である。なぜならば、ＨＡＳＨ＿ＩＮＳＴ＿ＳＷは、ＮＵＭ＿ＩＮＳＴ＿ＳＷから部分的に算定されるハッシュ関数値であるからである。さらにＮＵＭ＿ＩＮＳＴ＿ＳＷは、ＳＰＡＲＳＥ＿ＳＥＴに見出されなければならず、またＴＡＧ＿ＩＮＳＴ＿ＳＷのＮＡＭＥ＿ＳＷに付随しなければならない。

【０２９０】

ステップ４１２において検出された、確認されていない各タグＴＡＧ＿ＩＮＳＴ＿ＳＷｎに対してステップ４１７は、確認されないタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎに対するソフトウエアのインスタンス１１１～１１４に付随する使用管理方針ＰＯＬＯＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）に基づいて特定の報復措置を作る。この場合の報復措置は、ユーザー装置１０４の機能を停止するためのインストラクションを含むことができる。ステップ４１７に定められた報復措置は、それがユーザー装置１０４に通信された後に実行されることに留意すべきである。

【０２９１】

ソフトウエアのインスタンス１１１～１１４に付随する使用管理方針ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）は、保護センター１０３（図２）に保持され、ソフトウエアベンダー１０１により作られる各種のソフトウエアのインスタンス１１１～１１４に対する使用管理の扱い方を保護センター１０３（図２）にインストラクトするために、必要に応じてソフトウエアベンダー１０１から提供されることができる。すなわち、ソフトウエアベンダー１０１は、ソフトウエアのインスタンス１１１～１１４を１０４～１０７（例えば料金として）に提供することができる。これらのインスタンス１１１～１１４に使用制限を実行するためにソフトウエアベンダー１０１は、インスタンス１１１～１１４に対する方針ＰＯ

ＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）を作り出すことができる。呼び出し手順中保護センターは、方針ＣＡＬＬ＿ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）を実行するか、または取り締まる。前記に代わる実施形態としてソフトウエア（すなわち１１１）のインスタンスに対する方針は、１１１および１１２が同じソフトウエア内容をもつと仮定すると、その同じソフトウエアのその別のインスタンス（すなわち１１２）とは相違することが考えられる。これにより本発明は、使用管理を、例えば同じプログラムの２つのユーザーに対して別々に実行することが可能である、なぜならば各インスタンスは独自の付随タグをもち、呼び出し方針はインスタンスごと、またはユーザーごとに別々に維持されることができるからである。

【０２９２】

いずれの場合にも保護センター１０３（図２）においてタグテーブル２１０における各タグＴＡＧ＿ＩＮＳＴ＿ＳＷが真正であることを確かめられ（ステップ４１２）、または報復措置が確認されていない各タグに対して作成され（ステップ４１７）た後に、処理はステップ４１３に進み、このステップではタグテーブル２１０における確認された各タグＴＡＧ＿ＩＮＳＴ＿ＳＷｎが、タグをもつソフトウエアデータベース１３８（図９）に対比してチェックされる。本質的にステップ４１３は、ユーザー装置１０４に用いられたソフトウエアのインスタンス１１１～１１４に付随するタグテーブル２１０における各タグＴＡＧ＿ＩＮＳＴ＿ＳＷｎ（すなわち呼び出し処理を行うユーザー装置）は、ソフトウエアのインスタンスの使用管理方針ＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）にしたがって使用されている。各タグがステップ４１３においてテストされた後、処理はステップ４１４に進む。

【０２９３】

ステップ４１３において実行されるチェック処理は、多様な方法で行うことができる。１つの実施形態によればタグ付きのソフトウエアデータベース１３８（図９）は、タグＴＡＧ＿ＩＮＳＴ＿ＳＷｎと管理プログラム識別番号（２０９－Ａｓ）との間の結合のリストおよびこれらの結合が発見された時点を含む。この実施形態において確認プログラム（ＶＲＯ）３１５は、タグテーブル２１０のタ

グと同じタグ１２０（テーブル２１０のＣｏｌｕｍｎ１）が２つの装置にあるか否かを確かめるためのＴＡＧ＿ＩＮＳＴ＿ＳＷ＿ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥ＿ＣＡＬＬＵＰ＿ＴＩＭＥ結合のリストに対して比較することができる。タグ１２０がいくつかのＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥｓに付随することが判明する時には、報復措置をステップ４１８において作ることができる。

【０２９４】

本発明の好ましい実施形態においては、保護センターの確認プログラムＶＲＰ３１５は、タグ１２０　ＴＡＧ＿ＩＮＳＴ＿ＳＷと関連したデータ構造体（図１０の３２０，３２１）を採用しており、タグ１２０と関連したソフトウエアのインスタンス１１１～１１４が、呼び出し中のユーザーの装置１０４において、ソフトウエアのインスタンス１１１～１１４に対し指定された使用管理ポリシーＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）と一致して使用されているかをチェックする。もし、２つの異なるユーザーの装置（例えば、１０４と１０５）にはありえない、同一のソフトウエアのインスタンスが、（すなわち同一のタグが）、同時に使用可能な状況（例えば、ＵＳＡＧＥ　ＳＴＡＴＵＳ＝ＣＯＮＴＩＮＵＥＤ）にあることを、使用管理ポリシーが指定すると、そのタグのための呼び出し記録３２１中の詳細なデータが、ＶＲＰ３１５によるポリシー違反があったかのチェックを可能にする。

【０２９５】

タグテーブル２１０中の各タグ１２０　ＴＡＧ＿ＩＮＳＴ＿ＳＷが、ステップ４１３でチェックされると、タグテーブル２１０中のタグ１２０は、それらのタグと関連して指定されている報復措置と関係することがある。もし、不正にコピーされたタグ、または、使用管理ポリシーと一致して使われていないタグのために、報復措置が指定されると、処理はステップ４２０に進み、そこで、保護センター１０３（図２）中の確認プログラムＶＲＰ３１５が、指定された報復措置を用意し、継続メッセージ（ＣＭ）２１２を介して、ユーザーの装置１０４に送り返す。このような継続メッセージ（ＣＭ）２１２は、ユーザーの装置１０４に報復措置を課すために用いられ、ポリシーＰＯＬＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）違反でのタグテーブル２１０中のすべてのタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎのＵ

ＳＡＧＥ　ＳＴＡＴＵＳ領域のための“ＧＣ＿ＤＩＳＡＢＬＥＤ”措置値を含んでいる。

【０２９６】

タグ付けされたソフトウエアのもう１つの扱いでは、上述のタグ処理は、タグテーブルの一部においてのみなされる。例えば、アクセス（すなわち、使われようとしているソフトウエアのインスタンス）を要求しているユーザーの装置１０４～１０７（すなわち、ユーザーの装置の管理プログラム２０９）に対するタグについてのみ、処理がなされる。この場合、継続メッセージ２１２は、保護センター１０３（図２）で処理されたタグに関連したソフトウエアのインスタンスについてのみ、継続または報復措置を指定する。

【０２９７】

さらに他の実施形態では、購入されて無制限に使用されるソフトウエアに対して、タグ処理は全く必要とされず、これにより、ステップ３７２（図１２）に関連した措置がなくなる。代わりに、ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥのみが、確認される必要がある。この場合、ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥ（図６の上の列）は、ＩＤ＿ＴＡＧ＿ＴＡＢＬＥおよび事象履歴を含む（図６）。この実施形態では、各タグ１２０は、ＨＡＳＨ＿ＳＷ，ＮＡＭＥ＿ＳＷおよびＮＵＭ＿ＩＮＳＴ＿ＳＷに加えて、ＩＤ＿ＴＡＧ＿ＴＡＢＬＥを含んでいる。ＩＤ＿ＴＡＧ＿ＴＡＢＬＥ値は、購入時にタグ１２０（第１欄）に書き込まれ、図３Ａ，３Ｂおよび３Ｃ中のステップ１５３のハッシュ関数における独立変数となり、つまり、ＨＡＳＨ＿ＩＮＳＴ＿ＳＷになる。ＩＤ＿ＴＡＧ＿ＴＡＢＬＥはＩＤ（ＳＰ）２０９－Ａを含み、ＩＤ（ＳＰ）２０９－Ａが、装置１０４が最初に起動されたときに、例えばミリ秒値の時間を含む複製値に基づくことはごくまれであるので、各ＩＤ＿ＴＡＧ＿ＴＡＢＬＥ値は、権利侵害のない１つの現実の装置にのみ生じる。

【０２９８】

ディスクイメージのコピーという形態で権利侵害が起こると、１つのＩＤ＿ＴＡＧ＿ＴＡＢＬＥ値がいくつかの現実の装置に生じる（「双子」になる）が、装置１０４のＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥのＬＡＳＴ＿ＣＡＬＬＵＰ＿ＴＩ

M領域と、保護センター１０３（図２）の認証データベース１３８（図９）のＣＡＬＬＵＰ＿ＲＥＣＯＲＤのＣＡＬＬＵＰ＿ＴＩＭＥとが、呼び出し時に一致せず、ＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥでの確認が失敗する。これにより、保護センター１０３は、２つの呼び出しメッセージが２つの別々に構成された装置１０４～１０７から送られた場合には、報復措置をとる。

【０２９９】

さらに、２つの装置１０４～１０７は、同一の呼び出し手順を共有しようとすることもできない。なぜなら、それらのＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥｓは、それらのタグテーブル２１０それぞれのＨＡＳＨ（ＥＶＥＮＴ＿ＨＩＳＴＯＲＹ）領域によって異なるからである。そのハッシュ関数値が継続メッセージに送られるので、装置１０４から１０７のうち１つのみが、継続メッセージ２１２を適切に処理できる。２つの装置が複製により動作する場合には、管理プログラム２０９は、このように複製が企てられたことを認識し、報復措置をとる。したがって、各ＩＤ＿ＴＡＧ＿ＴＡＢＬＥは、ただ１つの装置１０４～１０７にあり、または関連し、でなければ、呼び出しは失敗する。タグがＩＤ＿ＴＡＧ＿ＴＡＢＬＥを含むとき、装置１０４～１０７の管理プログラム２０９は、タグ１２０に関連したソフトウエアのインスタンス１１１～１１４が、タグ１２０のＩＤ＿ＴＡＧ＿ＴＡＢＬＥ値が適切な装置のそれと一致する場合にのみ、使用されることを許容する。結果として、各ソフトウエアのインスタンス１０４～１０７は、ただ１つの装置１０４～１０７でのみ使用され、その装置は、タグ１２０のＩＤ＿ＴＡＧ＿ＴＡＢＬＥ値と一致するＩＤ＿ＴＡＧ＿ＴＡＢＬＥ値をもつ。

【０３００】

ステップ４１４において、確認プログラム（ＶＲＰ）３１５は、タグのないソフトウエアのインスタンスに対してタグテーブル２１０にエントリーがないか、決定する。ユーザーの装置１０４～１０７にインストールされた、タグのないソフトウエアのインスタンスは、特別のタグＵＮＴＡＧＧＥＤ＿ＳＷで示され、タグのないソフトウエアのためのＵＳＡＧＥ　ＳＴＡＴＵＳ欄は、ＵＮＴＡＧＧＥＤにセットされる。このＵＮＴＡＧＧＥＤ＿ＳＷタグエントリーは、好ましくは、ソフトウエアを作成したユーザーによるインストールまたは最初の使用の際に

なされ、指紋処理は、好ましくは、図７で説明するように、タグのないソフトウエアの最初の検出時に、ユーザーの装置１０４により実行される。

【０３０１】

図１３Ａにおいて、確認プログラム（ＶＲＰ）３１５が、ステップ４１４でタグテーブル２１０にタグのないエントリーを検出すると、ステップ４１５が実行される。ステップ４１５の処理では、ステップ４１０で保護センター１０３に転送された指紋テーブル１２６から、各指紋リストを得る。指紋テーブル１２６は、タグのないソフトウエアのインスタンスそれぞれについての指紋のリストからなる。確認プログラム（ＶＲＰ）３１５は、指紋テーブル１２６中の各指紋リストX_iと、指紋データ構造体１３７中のすべての指紋リストY_jとを、ＧＣＤＢ３００において、前述したように、一般ロケーション指紋チェックを用いて、付き合わせる。指紋リストX_iとY_jに指定された数よりも多く一致が見つかると、保護センターは権利侵害のソフトウエアの使用を検出して、処理はステップ４２０に進み、そこで、報復措置が用意され、呼び出しが実行されたユーザーの装置１０４に送られる。権利侵害のソフトウエアの権利侵害でないバージョンを作成したソフトウエアのベンダー１０１にも、通知される。

【０３０２】

各指紋リストX_iを保護センター中のすべての指紋リストY_jと比較するのは、コンピューターにとって負担が大きく、これは呼び出し中最も負担の大きい処理なので、ある実施形態では、これをいくぶん異なる方法で行う。この実施形態では、反転保護指紋テーブルと呼ばれる指紋リストが作成され、すべての権利侵害のソフトウエアのすべての指紋を含むが、複製された指紋は含まない。この反転保護指紋テーブルを用いて、保護センター１０３は、各リストX_iを調べ、リスト中いくつの指紋が、反転保護指紋テーブル（指紋データ構造体１３７として保持されている）中の指紋と一致するかを決定する。指定されたのよりも多くの一致が見つかると、各Y_jに対しX_iの詳細なチェックがなされ、指紋数においてごく近い一致があったか否かの決定がなされる。ステップ４１５で一致する指紋リストが検出されない場合には、ステップ４１９の処理に進み、前のステップ４１１または４１２で報復措置が規定されていないかを決定する。規定されてい

れば、処理は、前述したように、ステップ４２０に進む。

【０３０３】

ステップ４１９で報復措置が規定されていない場合には、ステップ４２１に進む。このステップでは、保護センター１０３に知らされたすべてのタグＴＡＧ＿ＩＮＳＴ＿ＳＷｎを、ペイパーユース（使用ごとに支払う）タグとして扱う。すなわち、保護センター１０３は、タグ付きのソフトウエアデータベース１３８（図９）に、ペイパーユース基準に基づいて課金されるべきソフトウエアのインスタンス１１１～１１４すべてのリストを保持できる。ステップ４２１では、そのようなタグ（第１欄）すべてについて、および１以上のペイパーユースタグの検出について、タグテーブル２１０を調べ、ステップ４２１は、保護センター１０３に、ペイパービューまたはペイパーユース１１１～１１４の使用特性に関して、会計情報（図示しない）をソフトウエアベンダー１０１に向けて送らせる。タグテーブル２１０中のタグエントリーのＲＵＮ　ＣＯＵＮＴまたはＵＳＥ　ＴＩＭＥ領域は、ペイパーユースの統計の決定に用いることができる。ペイパーユースタグが期限切れになると、ＴＡＧ＿ＩＮＳＴ＿ＳＷｎのためのＵＳＡＧＥ　ＳＴＡＴＵＳ領域は、“ＧＣ＿ＤＩＳＡＢＬＥＤ”にセットされる。これは、タグに対し使用禁止措置ＤＩＳＡＢＬＥ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）を用意することでなされる。使用禁止措置は、後述するように、継続メッセージ２１２に組み込まれる。

【０３０４】

ステップ４２１のペイパーユース処理が完了すると、ステップ４２２が、タグテーブル２１０中の完全に確認されて期限切れでないタグすべてに対し、継続措置ＣＯＮＴＩＮＵＥ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）を生成する。この継続措置は、継続メッセージ（ＣＭ）２１２に組み込まれる。

【０３０５】

ステップ４２３において、確認プログラム３１５は、継続メッセージ（ＣＭ）２１２を用意し、ユーザーの装置１０４に返送する。継続メッセージ（ＣＭ）２１２は、いくつかの領域を含んでいる。ＴＩＭＥ領域は、クロック３０４からの現在時刻を示し、ＩＤ＿ＴＡＧ＿ＴＡＢＬＥ領域は、呼び出しＨＡＳＨ（ＥＶＥ

ＮＴ＿ＨＩＳＴＯＲＹ）と同時の事象履歴のエンコードと同様に、もとは呼び出し処理のステップ４１０で保護センター１０３に送られたタグテーブル２１０の個別の確認を示す。ＡＣＴＩＯＮ領域は、特別のユーザーの装置１０４の管理プログラム（ＳＰ）２０９に対して利用可能な措置のリストから選択された措置ＡＣＴＩＯＮＳ＝（ＡＣＴＩＯＮＳ１，ＡＣＴＩＯＮＳ２，．．．ＡＣＴＩＯＮＳＮ）のリストを含む。ハッシュ関数値は、措置ＨＡＳＨ（ＡＣＴＩＯＮＳ）にも含まれ、計算される。最終的に、継続メッセージ２１２の完全な内容におけるデジタル的に署名された値は、継続メッセージ２１２が保護センター１０３になりすますサイトやホストにより偽造されないことを確実にするために、含まれる。好ましくは、署名された値は、次のように表される。

【０３０６】

ＳＩＧＮ＿ＧＣ（ＴＩＭＥ，ＩＤ＿ＴＡＧ＿ＴＡＢＬＥ，ＨＡＳＨ（ＡＣＴＩＯＮＳ），ＨＡＳＨ（ＥＶＥＮＴ＿ＨＩＳＴＯＲＹ））

【０３０７】

継続メッセージ（ＣＭ）２１２の領域のすべてが完成すると、確認プログラム３１５は、継続メッセージ（ＣＭ）２１２を、ステップ４１０で呼び出しを始めたユーザーの装置１０４内の管理プログラム（ＳＰ）２０９に、安全に返送または返信する。１つの実施形態では、これには、呼び出し中に装置により与えられた公開のキーを使う。侵害者が同じ公開のキーをもつ２つの装置を設定しても、正しい事象履歴をもつ１つの装置のみが、本発明のこの実施形態にしたがって、継続メッセージ２１２を処理できる。

【０３０８】

最終的に、ステップ４２５において、保護センター１０３は、呼び出し処理についての呼び出し記録ＣＡＬＬ－ＵＰ＿ＲＥＣＯＲＤｎを作成する。保護センター１０３は、このＴＡＧ＿ＩＮＳＴ＿ＳＷに関連するデータ構造体３２０（図１０）に、この呼び出し記録ＣＡＬＬ－ＵＰ＿ＲＥＣＯＲＤｎへのレファランスを付加する。レファランスは、メモリーポインターかＣＡＬＬＵＰ＿ＲＥＣＯＲＤの個別の識別子のいずれかである。呼び出し記録の内容については、図１０を参照して前述した。

【０３０９】

本発明のこの構成の有用性の例は、本発明の特徴のいくつかを明確にする。例えば、ユーザー２１３がソフトウエアのインスタンス１１１～１１４を使用する１年のライセンスを購入し、その１年の期限が切れた後、ユーザー２１３がライセンスを更新しないとする。ユーザー２１３が更新しないので、ソフトウエアベンダー１０１は、ユーザー２１３がもはやライセンスを保持していないソフトウエアのインスタンス１１１～１１４を使用禁止にすることを望む。本発明によれば、ベンダー１０１は、ソフトウエアのインスタンス１１１～１１４に関連する保護センター１０３にポリシーＰＯＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）を単に設定して、インスタンス１１１～１１４が備えられた装置１０４から保護センター１０３への次の呼び出しにおいて、インスタンスを使用禁止にできる。このようにして、強力な使用管理が、ユーザー２１３にソフトウエアのインスタンス１１１～１１４の返却を求めることなしに、なされる。ユーザー２１３が、後でライセンスの更新を希望するならば、ベンダー１０１は、ただ保護センター１０３でポリシーＰＯＩＣＹ（ＴＡＧ＿ＩＮＳＴ＿ＳＷ）を変更すればよく、そうすると、次の呼び出しが、ユーザーの装置１０４のタグテーブル２１０を、インスタンス１１１～１１４について“ＣＯＮＴＩＮＵＥＤ”ステータスタグＴＡＧ＿ＩＮＳＴ＿ＳＷとして更新する。

【０３１０】

保護センター１０３に用意された継続メッセージＣＭ２１２の種々の要素、および、ＣＭ２１２に組み込まれた前述のデジタル署名は、本発明の実施形態でいくつかの重要な目的を果たす。継続メッセージ２１２は、それを受けるユーザーの装置１０４の管理プログラム２０９に、装置のタグテーブル２１０のＵＳＡＧＥ　ＳＴＡＴＵＳ欄をどう更新するか、および、もしあるなら、どの報復措置をとるか、について指示する。識別ハッシュ関数およびＣＭ２１２（図１３Ｂの４２３）の他の値は、要求された呼び出し処理を完遂するために、不正なユーザー２１３が、ユーザーの装置１０４（すなわち、１０４～１０７のうちの１つ）からの現在の呼び出しに応じて保護センター１０３により実際に与えられた１つ以外のあらゆる継続メッセージ２１２を使用することを、仮想的に不可能にする。

また、敵対者や敵対ホストは、不正ＣＭ２１２を装置１０４に送ることによって、ユーザーの装置（すなわち、１０４）へのサービスを拒否するような損害を与えることはできない。

【０３１１】

前記の好ましい実施形態で述べたように、本発明は、ソフトウエアベンダー１０１により作成され、配布された（すなわち、販売された）ソフトウエアのインスタンス１１１～１１４、または、ユーザーの装置１０４によるアクセスで権利侵害され、不正に配布されたインスタンスの使用を、検出し、制御し、かつ管理する機構を提供する。各ソフトウエアのインスタンス１１１～１１４を個別に識別する、偽造できず、認証されたタグＴＡＧ＿ＩＮＳＴ＿ＳＷを与えることにより、使用管理がなされる。好ましい実施形態では、ＴＡＧ＿ＩＮＳＴ＿ＳＷが適正にソフトウエアのインスタンスＩＮＳＴ＿ＳＷに関連しているかを確認するのに、指紋位置の同一性（same location fingerprinting）を用いる。

【０３１２】

指紋は、やや異なる目的にも同様に用いることができる。そのような１つの目的は、オペレーティングシステム２０７のテキストの完全性（textual integrity）のチェックである。これは、プログラムの一部に、他の部分または他のプログラムを前記指紋処理でチェックさせることにより、なしえる。これは、例えば管理プログラム２０９やオペレーティングシステム２０７の不法変更を防止する。他の実施形態では、電子的にプログラム可能なリードオンリーメモリーのような外部ハードウエアが、機器または装置１０４～１０７の電源が入っているときに、このチェックを行える。いずれの場合も、チェックプログラムは、前述のように、オペレーティングシステムプログラム２０７のいくつかの部分でハッシュ指紋を計算でき、例えば、指紋の不一致を見つけると、装置の失敗を起こす。また、指紋は、オペレーティングシステム２０７により管理プログラム２０９テキストをチェックするのにも、用いることができる。同様に、管理プログラム２０９は、事象履歴のハッシュを確認または認証のチェックに用いることができる。

【０３１３】

これは、例えば、以下のように動作する。管理プログラム２０９は、ＭＤ５の

ような増大ハッシュ関数法を用いて、タグテーブル２１０のデータのハッシュを各更新の後に更新できる。タグテーブル２１０を新しい事象で更新する前に、定期的に、管理プログラム２０９は、保持するハッシュ関数値がタグテーブル２１０のハッシュと等しいことを確認できる。これらのチェックのいずれかでも失敗すると、管理プログラム２０９またはオペレーティングシステム２０７は、報復措置をとることができる。このように、本発明の構成は、本発明自体として動作するソフトウエアを不法変更する装置またはソフトウエアを検出するために、用いることができる。

【０３１４】

指紋のさらなる用途は、ソフトウエアのインスタンス１１１～１１４のタグ１２０に対する要求に応じてタグサーバー１０２に出された特定のベンダーソフトウエアが、他の適法なベンダーのソフトウエアＳＷからの不法な複製または派生物でないことの確認である。そのような行為が可能とすると、侵害者であるベンダーが、認証されたタグ１２０を供給したタグサーバー上の、他の適法なベンダーのソフトウエアＳＷを配布するのを許すことになる。本発明のこの構成は、あらたに生成したソフトウエアを指紋付けし、一般位置指紋（general location fingerprinting ）を用いて、新たなソフトウエアを既存のソフトウエアと比較し、新たに出されたベンダーソフトウエアが適法なベンダーソフトウエアＳＷに酷似していないかを調べて、このような形態の侵害を防止する。

【０３１５】

ソフトウエアのインスタンス１１１～１１４は、それがインストールされるときまたは最初に使用されるときにチェックされたタグをもっている。タグは、また、後にもチェックされる（すなわち、ハッシュ、署名または呼び出し処理を介して）。ソフトウエアが最初に使用されるまで待つ理由の１つは、ソフトウエアが大容量の場合、最初にインストールされるときよりも、ソフトウエアの実行中の方が、チェックの負担が少ないからである。

【０３１６】

失敗を理由に、装置の状態（ステータス）は、前の状態に再構築される。この場合、ユーザー２１３は、古いＨＥＡＤＥＲ＿ＴＡＧ＿ＴＡＢＬＥを送ってもら

う必要があることを通知するために、保護センター１０３に連絡しなければならない。この特典を受けるにつき疑わしいユーザーは、保護センター１０３に容易に追跡される。

【０３１７】

図１４は、本発明の他の実施形態で用いられるデータ構造体を示し、この実施形態によれば、保護センター１０３が共有データファイルを供給するソフトウエアを呼び出すことを不要にできる。ワープロのプログラムを例にとる。ワープロのファイルと同様に、ワープロのソフトウエアも、知人間でよく交換される。一般的には、最初のケースは許されるが、２番目のソフトウエアプリケーション交換のケースは許されない。このような権利侵害を防止するために、本発明の実施形態は、図１４のデータ構造体６００に示すように、例えばＩＤ＿ＴＡＧ＿ＴＡＢＬＥ同様に、プログラムに付随するＴＡＧ＿ＩＮＳＴ＿ＳＷ１２０を書き込み、各共有ファイルの不明な位置（invisible location）への最近のアクセス時刻を書き込んで、ソフトウエアプリケーションプログラムを変更できる。また、同図に示すように、プログラムは、ＴＡＧ＿ＩＮＳＴ＿ＳＷおよびＴＡＧ＿ＴＡＢＬＥ６０１への最近のアクセス時刻を書き込む。

【０３１８】

共有データファイル（すなわち、例えばドキュメントで、ここではＳＳＤで参照される）中の不明な位置（すなわち、ユーザーにとって不明な）に蓄積されたデータ構造体６００は、共有ソフトウエアデータＳＳＤファイルのコメントセクションに置かれ、好ましくは３つの独立変数を用いる偽造できないハッシュ関数に付随できる。

【０３１９】

図１５は、前述のソフトウエア権利侵害保護機構を提供する本発明の実施形態のステップを示す。図１５のステップ７００において、ＩＤ＿ＴＡＧ＿ＴＡＢＬＥ　Ｘをもつ第１のユーザーの装置（すなわち、ユーザーの装置１０４）の管理プログラムＳＰ　２０９が、共有ソフトウエアデータＳＳＤへのアクセスを検出すると、管理プログラム２０９は、共有ソフトウエアデータＳＳＤと、ある特定の時刻にＴＡＧ＿ＩＮＳＴ＿ＳＷ　Ｔをもつソフトウエアのインスタンス（すな

わち、１１１～１１４のうちの１つ）によりアクセスされた共有ソフトウエアデータＳＳＤ内の所定の位置の記録とを調べる。そして、ステップ７０１で、ソフトウエアのインスタンス（潜在的に他の機械または他のユーザーの装置（例えば１０５）にある）が、共有ソフトウエアデータファイルＳＳＤを実行し、アクセスしようとすると、ユーザーの装置１０５の管理プログラム２０９は、共有ソフトウエアデータファイルＳＳＤ中にデータ構造体６００があることを検出し、ＳＳＤからタグＴを得て、ユーザーの装置１０５（共有ファイルを得ている装置、ただし、ファイルＳＳＤの装置を作製する必要はない）のタグテーブル２１０をチェックし、タグテーブル２１０にタグＴがあるかを調べる。タグＴがない場合は、共有ソフトウエアデータＳＳＤにアクセスするために第２の装置１０５（共有データを得ている装置）で使用されたソフトウエアのインスタンスは、複製されたものではなく、アクセスが認められてステップ７０３の処理に進む。

【０３２０】

一方、ステップ７０１で、共有ソフトウエアデータＳＳＤ中のデータ構造体６００にタグＴがある場合には、処理はステップ７０２に進む。ステップ７０２では、第２の装置１０５の管理プログラム２０９は、タグＴの付いたソフトウエアのインスタンス（例えば、第２の装置１０５のインスタンス１１１～１１４のうちの１つ）が、ＳＳＤに組み込まれたデータ構造体６００に示された時刻に共有データファイルを書き込んだかを調べる。書き込んでいなかった場合には、権利侵害が起こったのであり、管理プログラム２０９は、ステップ７０４で第２のユーザーの装置に対し報復措置を実行する。ステップ７０２で、第２の装置１０５の現在のソフトウエアのインスタンス１１１～１１４が、ＳＳＤに組み込まれたデータ構造体６００中の情報により示されたように、共有ソフトウエアデータＳＳＤにアクセスすることが決定されると、処理は７０３に進み、そこで、共有ソフトウエアデータへのアクセスが認められる。

【０３２１】

本発明の他の実施形態では、同じソフトウエアの異なるソフトウエアのインスタンスは、装置識別子によって異なる。このような実施形態の利点は、保護センターとの連絡の必要性が低減されることである。不利な点は、各ソフトウエアの

インスタンスは、異なっていなければならず（タグの有無まで対比して）、装置から装置へ移せないことである。この実施形態では、装置識別子は、利用できる場合にはプロセッサー識別子から作成されるか（インテル社製のペンティアム（登録商標）III のようなプロセッサーは、プロセッサー識別子をもっている）、好ましくは管理プログラム識別子から作成され、前述したようなプロセッサー識別子を組み込んでいる。各ソフトウエアのインスタンスは、テストでそのソフトウエアのインスタンスを使用する装置の識別子を、ソフトウエアのインスタンスのコードに組み込む。そのようなテストは、Ｃ言語で、例えば“ｉｆ文”として、表される。テストでは、組み込まれた識別子を装置識別子と比較する。ソフトウエアは、実行中、テストを行う。比較が成功（一致）すると、装置はソフトウエアのインスタンスを使用する。比較が失敗（不一致）であると、装置はインスタンスを使用せず、管理プログラムに報復措置をとるよう通知する。侵害未遂は、装置識別子をチェックしないように、プログラムを変更する。これは、タグ付きのソフトウエアを、あたかもタグなしで権利侵害であるかのようにするのに似ている。装置テストが変更され、または除去されたソフトウエアは、図１３Ａに詳述し、ステップ４１４から始まる指紋に基づく機構により検出される。

【０３２２】

この実施形態の変形では、ベンダーが、装置識別子と、装置識別子を組み込むソフトウエアのインスタンスのハッシュのデジタル署名との両方を送る。これは、次のように計算される。

【０３２３】

ＳＩＧＮ＿ＶＥＮＤＯＲ（ＨＡＳＨ＿ＩＮＳＴ＿ＳＷ）

ただし、ＨＡＳＨ＿ＩＮＳＴ＿ＳＷ＝ＨＡＳＨ（ＳＷ，ＤＥＶＩＣＥ＿ＩＤＥＮＴＩＦＩＥＲ）

【０３２４】

ここで、ＳＩＧＮ＿ＶＥＮＤＯＲは、ベンダーのデジタル署名であり、ＨＡＳＨ＿ＩＮＳＴ＿ＳＷは、ソフトウエアの内容（すべてのインスタンスに個別である）に組み込まれたＤＥＶＩＣＥ＿ＩＤＥＮＴＩＦＩＥＲを加えて計算される。装置識別子を組み込んだソフトウエアのインスタンスは、好ましくは、その識別

子を、ソフトウエアの内容の最初または最後に配置し、ハッシング処理の負担を軽減する。第２のテストでは、デジタル署名ＳＩＧＮ＿ＶＥＮＤＯＲが確認され、第３のテストでは、送られたＨＡＳＨ＿ＩＮＳＴ＿ＳＷが、ソフトウエアのインスタンスのハッシングの結果値に等しいかを確認する。これらのテストは、ユーザーの装置の管理プログラムで実行される。デジタル署名が認証されないか、ＨＡＳＨ＿ＩＮＳＴ＿ＳＷが、受けたソフトウエアのインスタンスのハッシュと異なる値をもつと、管理プログラムにより報復措置がとられる。

【０３２５】

以上においては、タグサーバー１０２、保護センター１０３およびベンダー１０１は、分離されたものとして説明した。他の実施形態では、これらの役割をまとめてもよい。例えば、１つのサイト、ネットワークホストまたはサーバーは、保護センター１０３およびタグサーバー１０２の両方として機能できる。あるいは、ソフトウエアベンダー１０１は、３つすべての役割を果たすことができる。さらにまた、各処理または役割を分離しても、前記実施形態における１つの要素（すなわち、タグサーバー、保護サーバー、ベンダー）に割り当てたいくつかの機能は、他の要素により実行できる。例えば、同一位置指紋（same-location fingerprinting）は、タグサーバー１０２に代わって、ベンダー１０１で実行できる。

【０３２６】

本発明を好ましい実施形態により図示し、説明してきたが、当業者には、前記特許請求の範囲で定まる本発明の精神と範囲から逸脱することなく、形状または細部の各種の変更が実行可能であることは理解されるであろう。

【図面の簡単な説明】

【図１】

本発明の一実施形態かかる情報システムの図である。

【図２】

本発明の一実施形態かかるシステムにおける情報の流れの詳細図である。

【図３Ａ】

本発明の一実施形態に従ってソフトウエアインスタンスに対して署名されたタ

グを作る処理ステップを示すフローチャートである。

【図３Ｂ】

本発明の一実施形態に従ってソフトウエアインスタンスに対して署名されていないタグを作る処理ステップを示すフローチャートである。

【図３Ｃ】

本発明の一実施形態に従ってソフトウエアインスタンスに対して指紋を持つ署名されていないタグを作る処理ステップを示すフローチャートである。

【図４】

本発明の一実施形態にかかるユーザー装置のアーキテクチャーを示す図である。

【図５】

本発明の一実施形態に従ってユーザー装置にベンダーソフトウエアをインストールする処理ステップを示すフローチャートである。

【図６】

本発明の一実施形態にかかるタグテーブルの内容を示す図である。

【図７】

本発明の一実施形態に従ってユーザー装置にタグのないソフトウエアをインストールする処理ステップを示すフローチャートである。

【図８】

本発明の一実施形態に従ってソフトウエアの使用管理を実施する本発明のシステムによって実行される高レベル処理ステップを示すフローチャートである。

【図９】

本発明の一実施形態にかかる保護センターのアーキテクチャーを示す図である。

【図１０】

本発明の一実施形態にかかるソフトウエアインスタンスに対する保護センター記録の内容を示す図である。

【図１１】

図１１は、ベンダーのソフトウエアに関するベンダーの権利を侵害するソフト

ウエアをベンダーが検出した際に、本発明の一実施形態にかかる保護センターによって実行される処理のフローチャートである。

【図１２】

本発明の一実施形態に従って保護センターに対する呼び出し手順を実行する際に、ユーザー装置の管理プログラムによって実行される処理ステップのフローチャートである。

【図１３Ａ】

本発明の一実施形態に従って実行される保護センター呼び出し処理ステップのフローチャートである。

【図１３Ｂ】

図１３Ａの続きのフローチャートである。

【図１４】

保護センターの呼び出しなしに、本発明の一実施形態で使用されるデータ構造体を示す図である。

【図１５】

保護センターの呼び出しなしに、本発明の一実施形態におけるユーザー装置の管理プログラムによって実行される処理ステップのフローチャートである。

【図１】

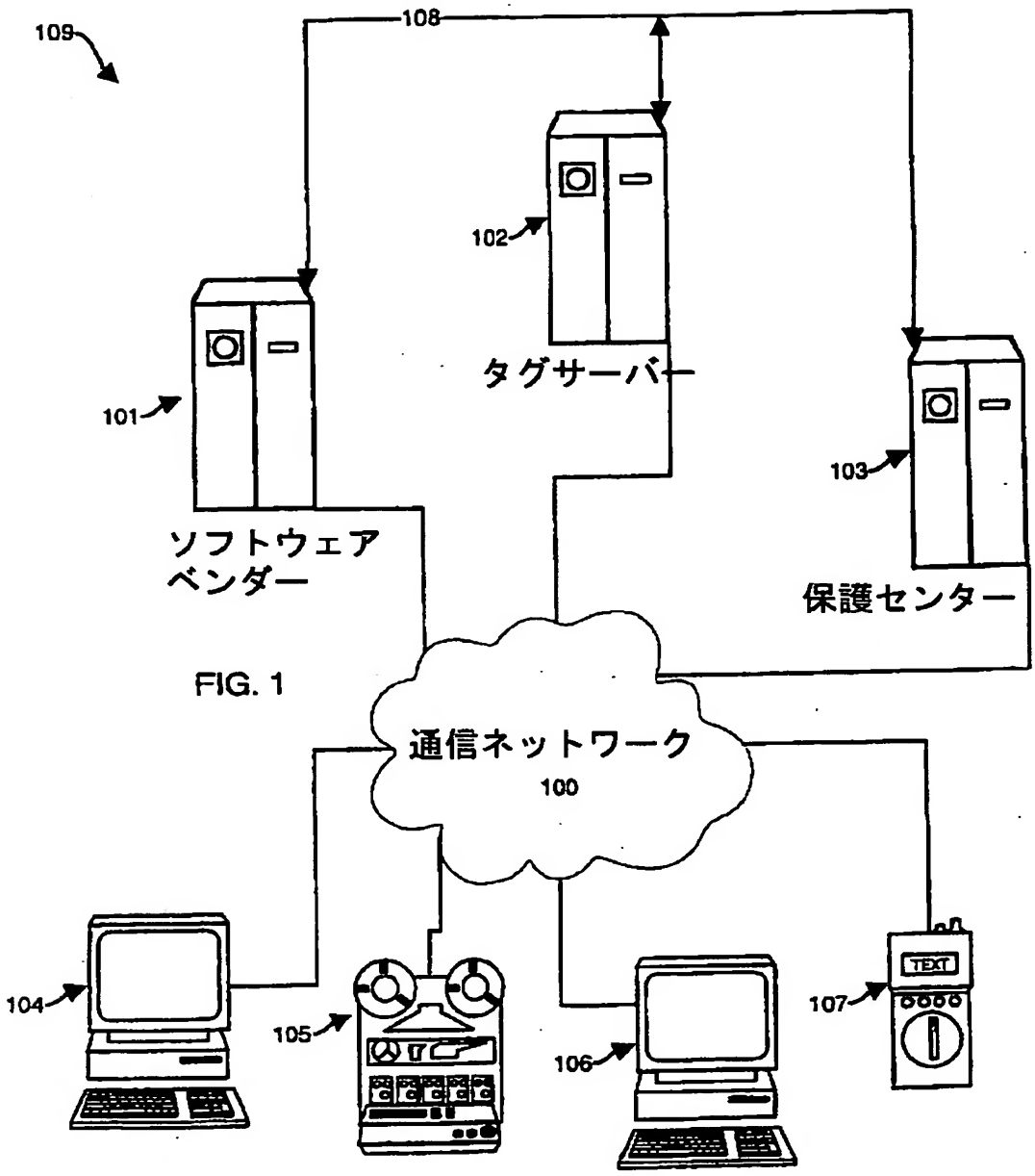
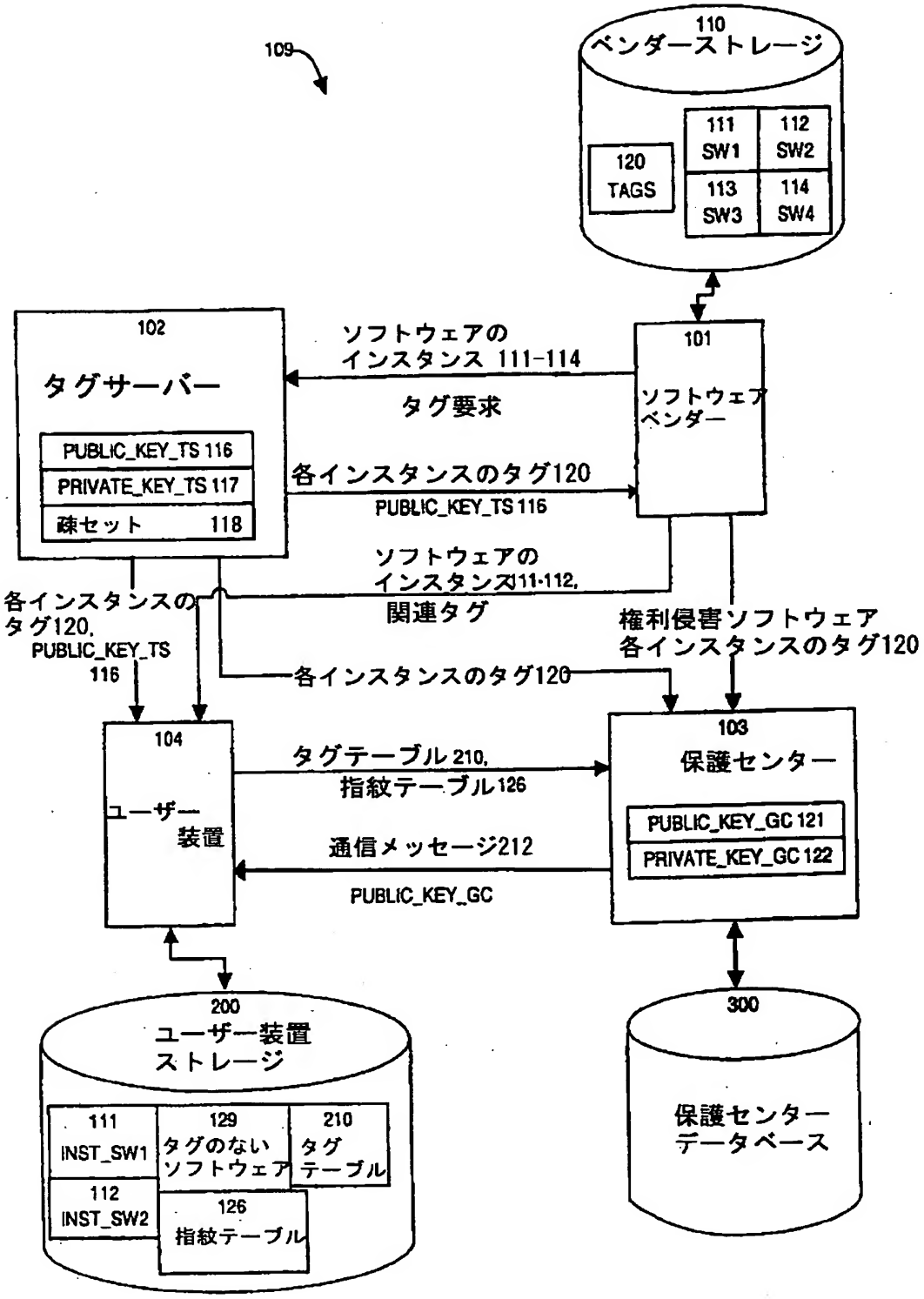


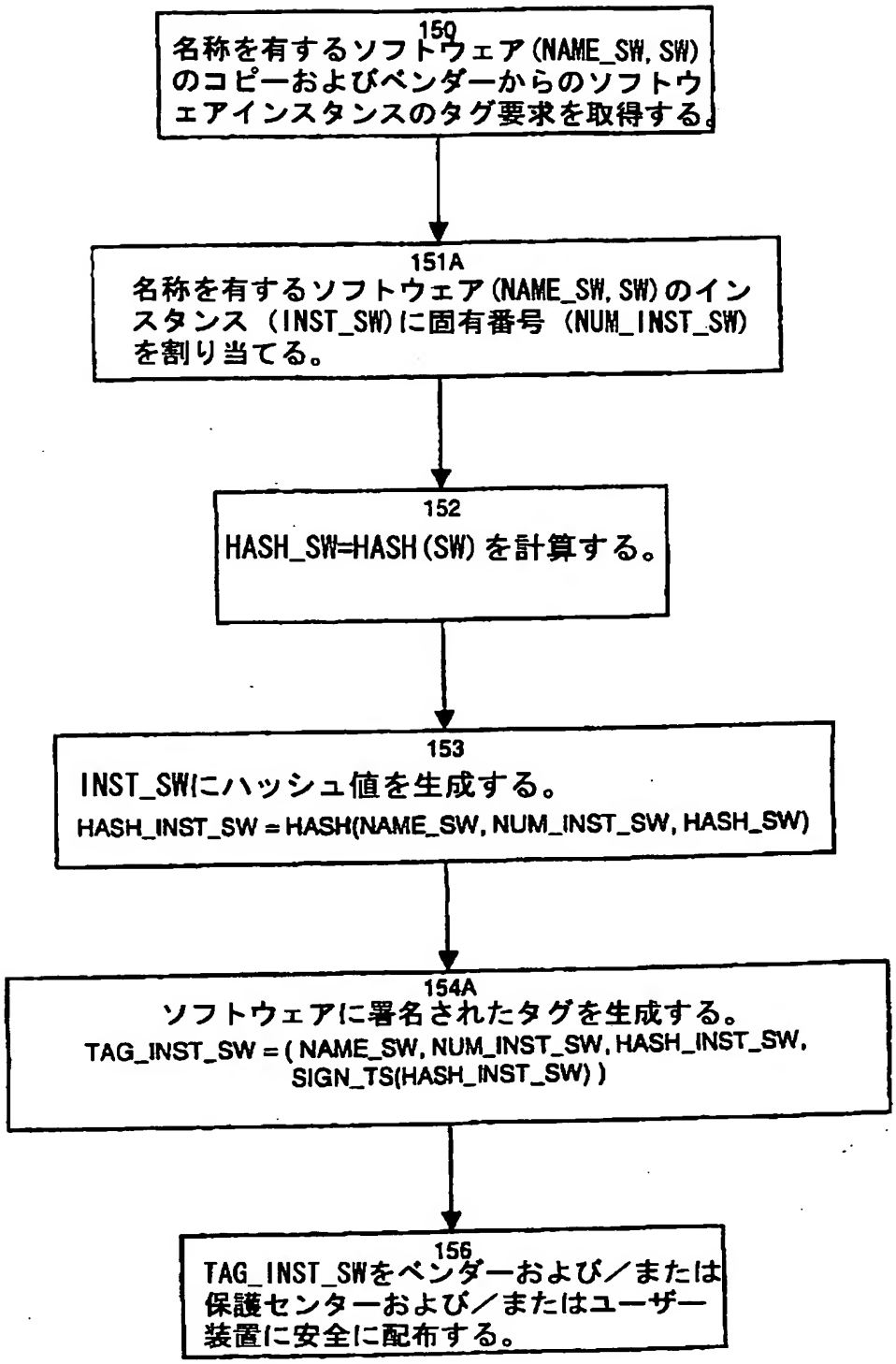
FIG. 1

ユーザー装置 104-107

【図２】

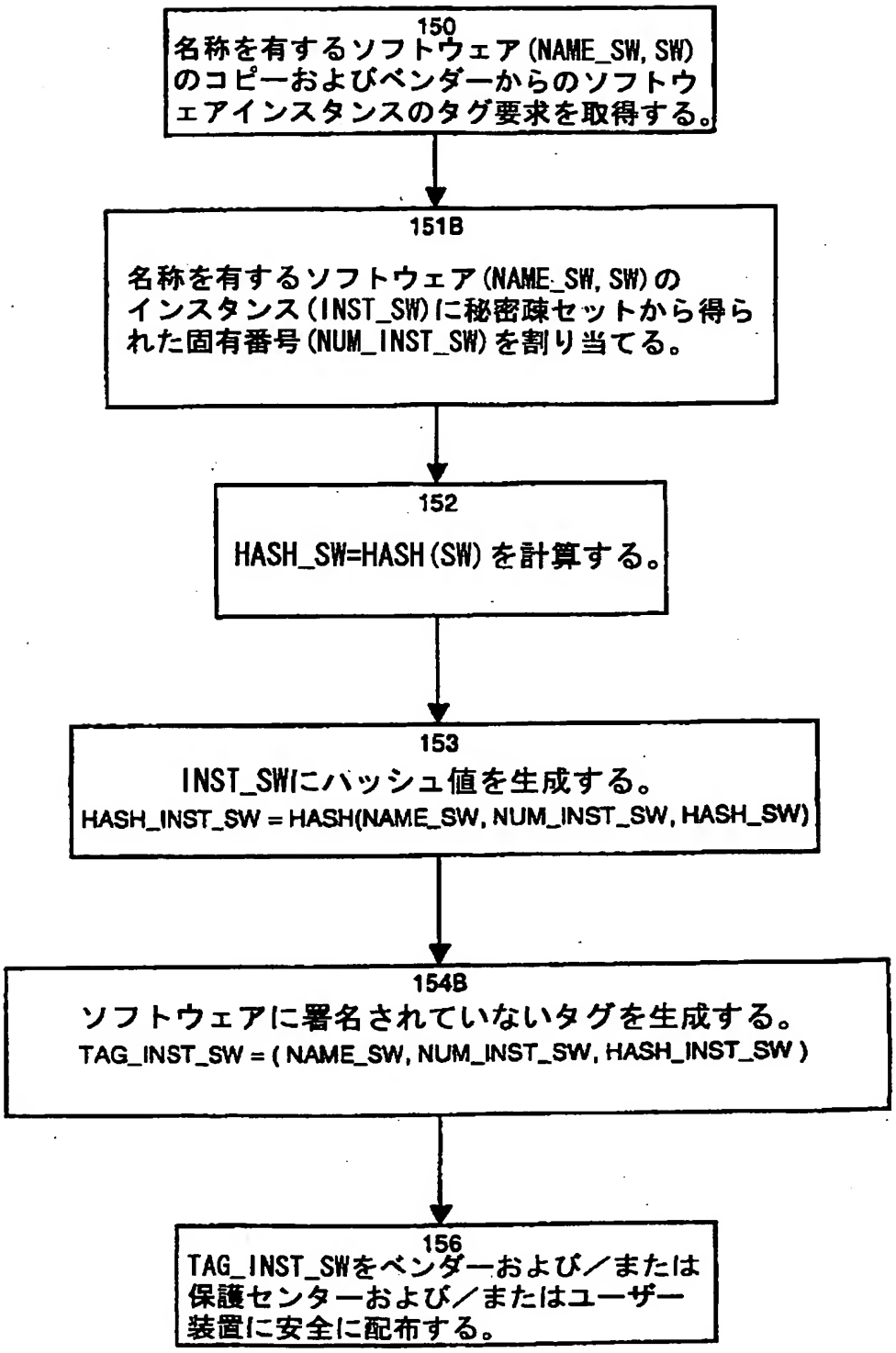

109
110
ベンダーストレージ
111
SW1
112
SW2
113
SW3
114
SW4
120
TAGS
102
タグサーバー
PUBLIC_KEY_TS 116
PRIVATE_KEY_TS 117
疎セット 118
ソフトウェアの
インスタンス 111-114
タグ要求
101
ソフトウェア
ベンダー
各インスタンスのタグ120
PUBLIC_KEY_TS 116
ソフトウェアの
インスタンス111-112,
関連タグ
各インスタンスの
タグ120,
PUBLIC_KEY_TS
116
各インスタンスのタグ120
権利侵害ソフトウェア
各インスタンスのタグ120
104
ユーザー
装置
タグテーブル210,
指紋テーブル126
103
保護センター
PUBLIC_KEY_GC 121
PRIVATE_KEY_GC 122
通信メッセージ212
PUBLIC_KEY_GC
200
ユーザー装置
ストレージ
111
INST_SW1
129
タグのない
ソフトウェア
210
タグ
テーブル
112
INST_SW2
126
指紋テーブル
300
保護センター
データベース

【図３Ａ】



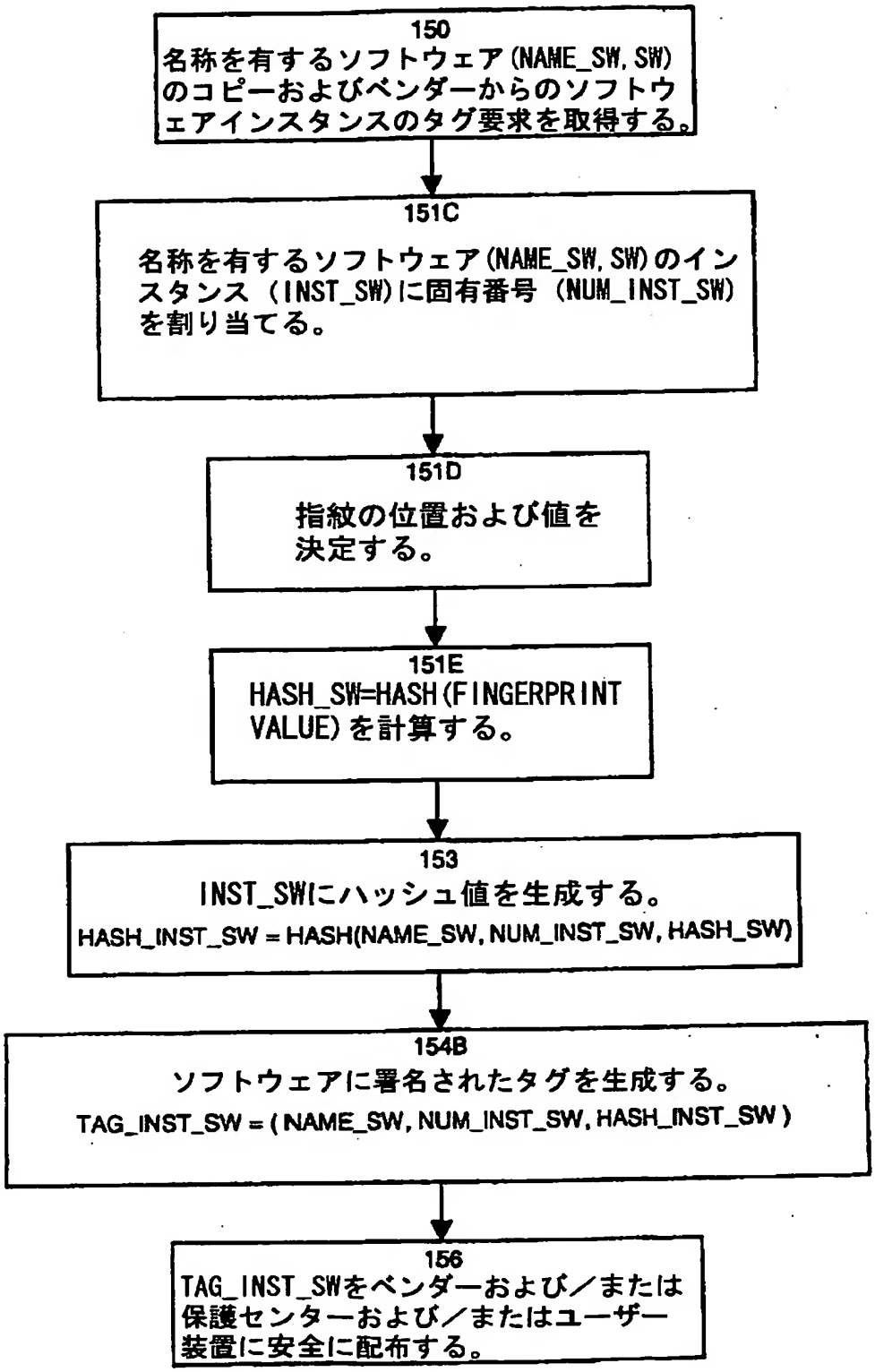
タグサーバーによる署名されたタグの生成

【図３Ｂ】



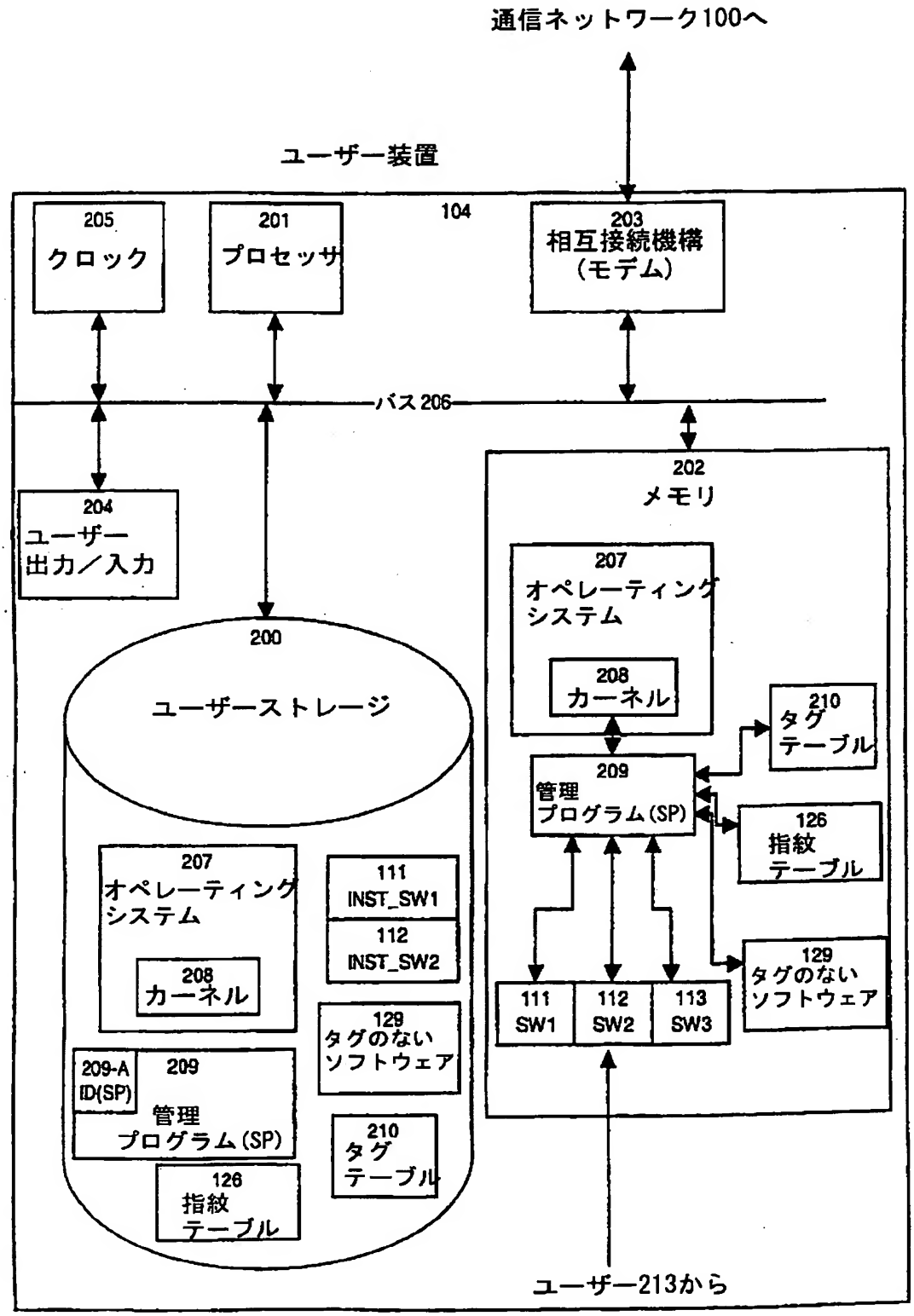
タグサーバーによる署名されていないタグの生成

【図３Ｃ】

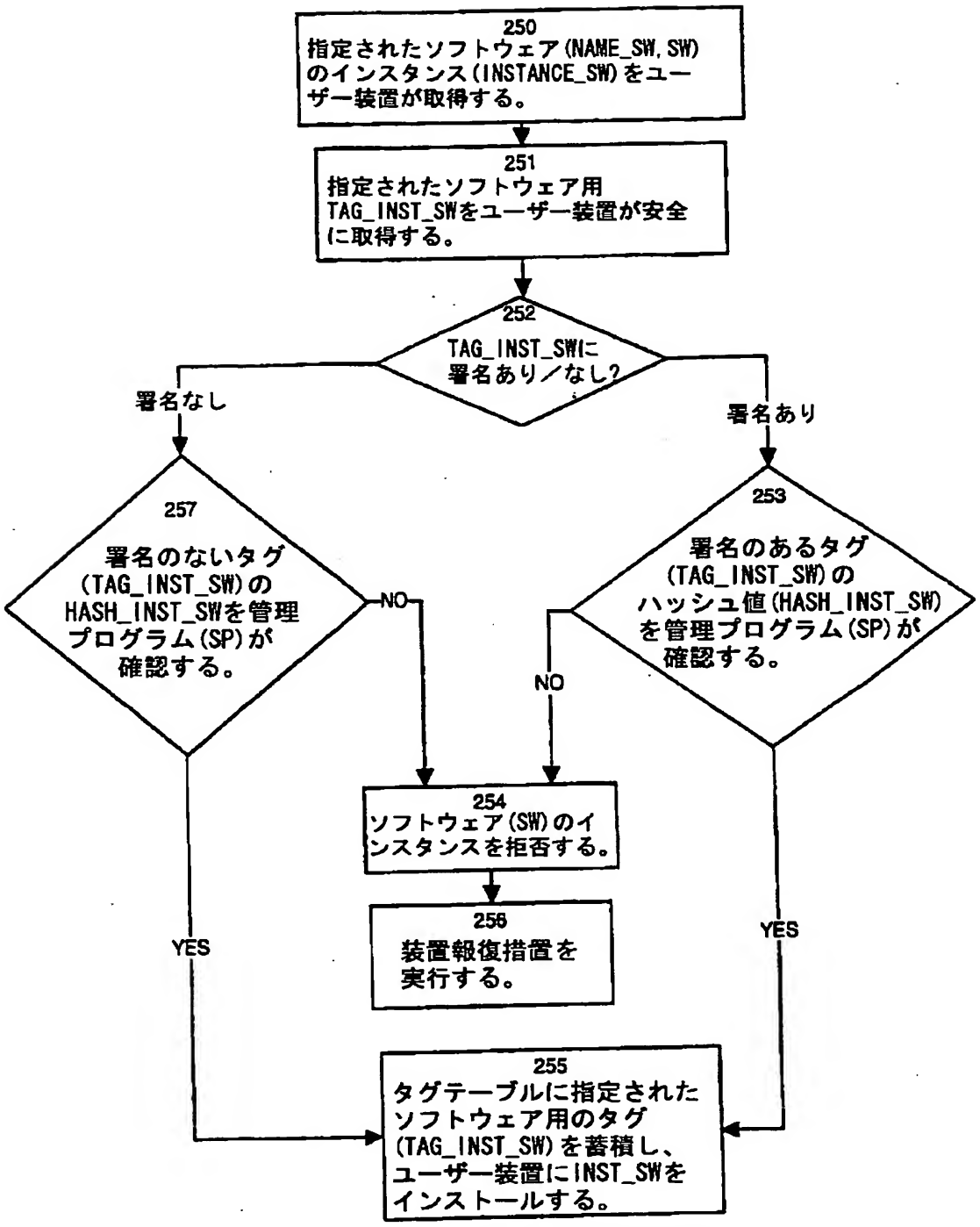


タグサーバーによる同一位置指紋を用いたタグ生成

【図４】


通信ネットワーク100へ
ユーザー装置
104
205
クロック
201
プロセッサ
203
相互接続機構
(モデム)
バス206
204
ユーザー
出力／入力
202
メモリ
207
オペレーティング
システム
208
カーネル
210
タグ
テーブル
209
管理
プログラム(SP)
126
指紋
テーブル
129
タグのない
ソフトウェア
111
SW1
112
SW2
113
SW3
200
ユーザーストレージ
207
オペレーティング
システム
208
カーネル
111
INST_SW1
112
INST_SW2
129
タグのない
ソフトウェア
209-A
ID(SP)
209
管理
プログラム(SP)
210
タグ
テーブル
126
指紋
テーブル
ユーザー213から

【図５】



ベンダーソフトウェア(SW)のタグのあるインスタンスをユーザー装置にインストール

【図６】

タグテーブル

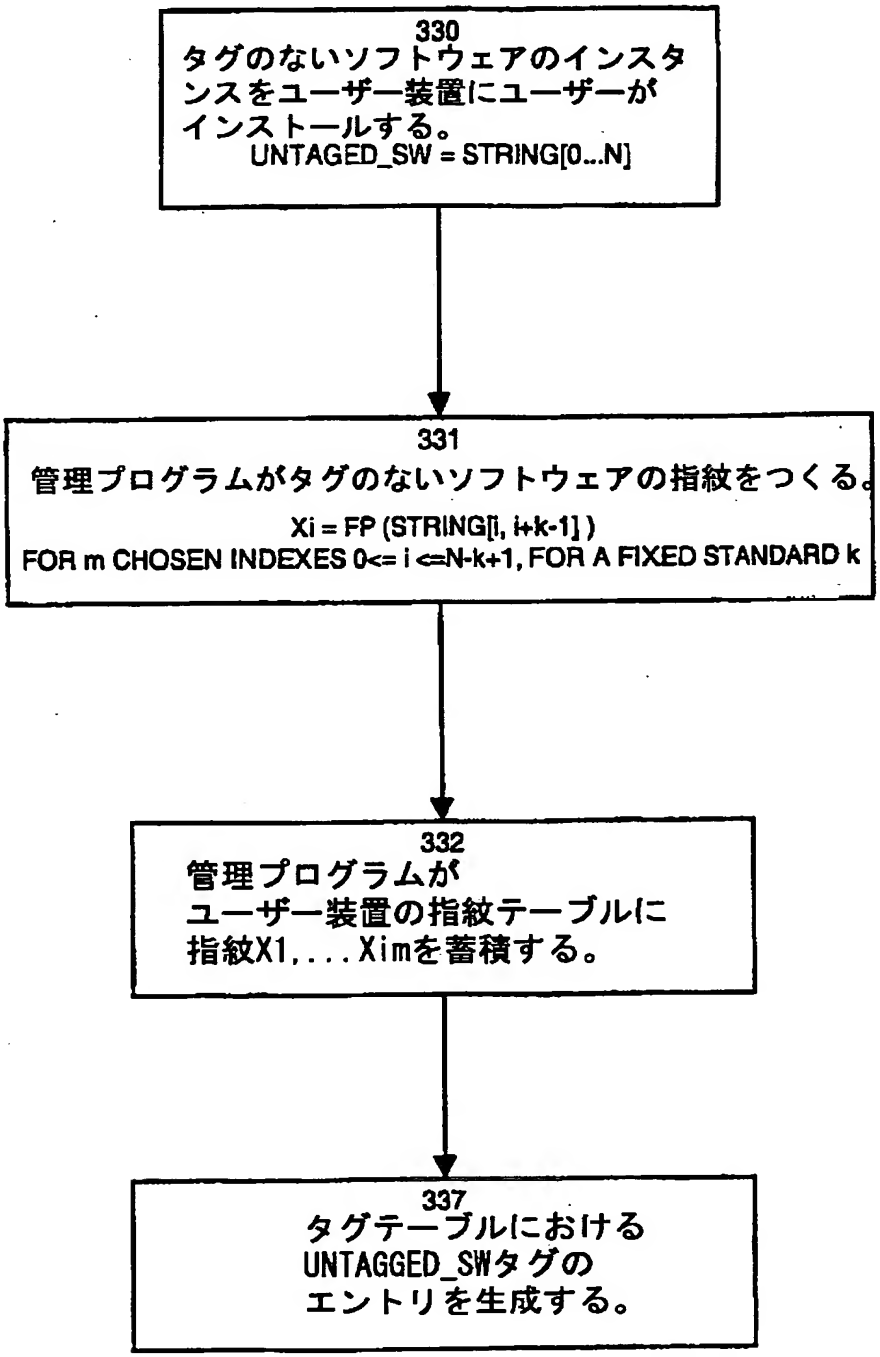
210				
HEADER_TAG_TABLE=(ID_TAG_TABLE, LAST_GC_CM, LAST_CALLUP_TIME, NUMBER_DEVICE_BOOTUPS)				
タグ	使用状況	動作時刻	ラン カウント	使用時間
TAG_INST_SW1	CONTINUED	11/22/98 11:02	10	00:58
TAG_INST_SW2	INSTALLED REMOVED	11/24/98 21:36 11/26/98 09:31	3	00:11
TAG_INST_SW3	GC_DISABLED	11/22/98 11:02	0	00:00
TAG_INST_SW4	CONTINUED	11/25/98 14:17	4	10:34
UNTAGGED_SW1	UNTAGGED	11/25/98 14:17	0	00:00

注：ID_TAG_TABLE = (ID(USER)*, ID(DEVICE)*, ID(PP)*, ID(OS)*)

* 不明の場合もある。

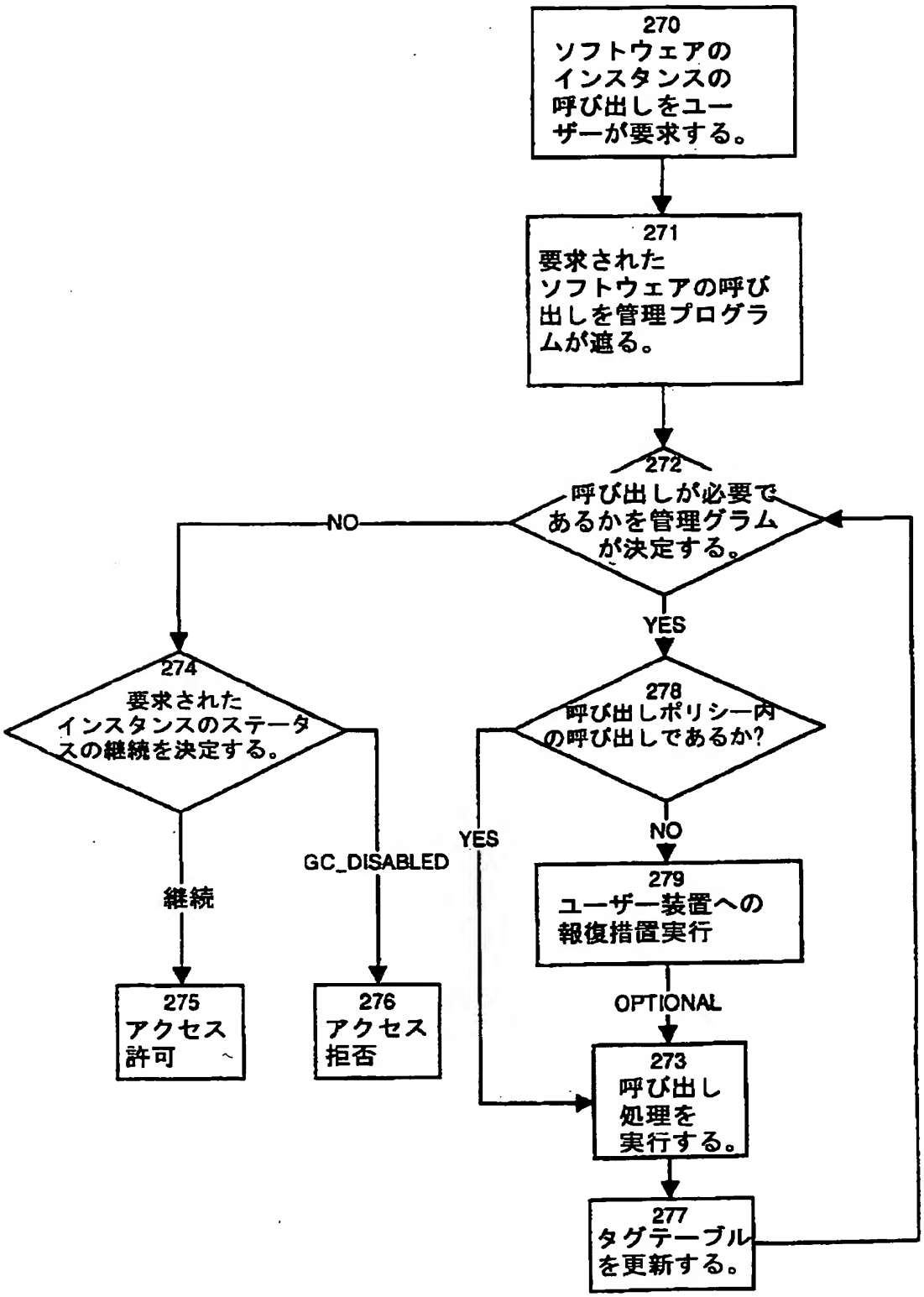
特表２００３－５００７２２

【図７】



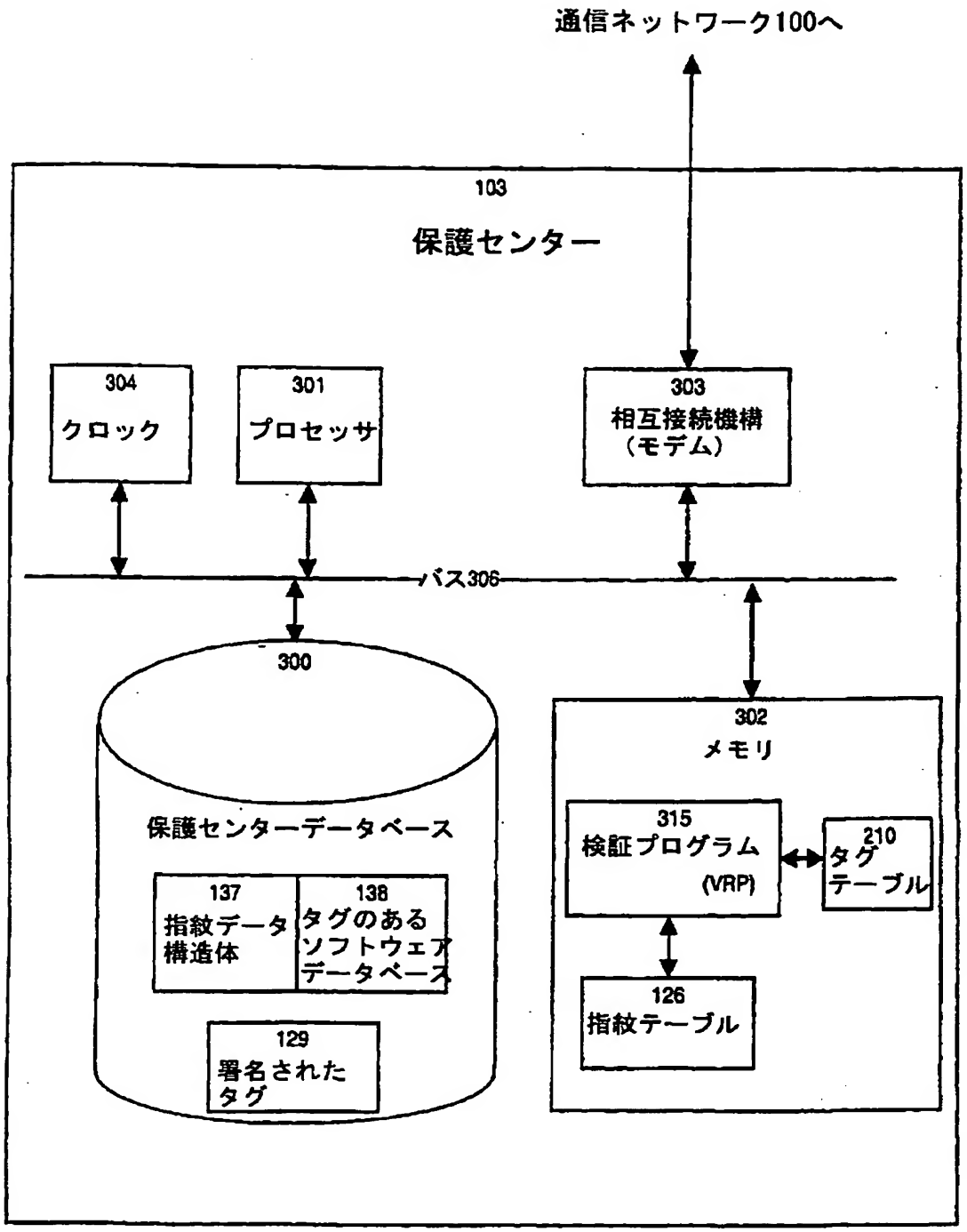
タグのないソフトウェア(UNTAGGED_SW)をユーザー装置にインストール

【図８】

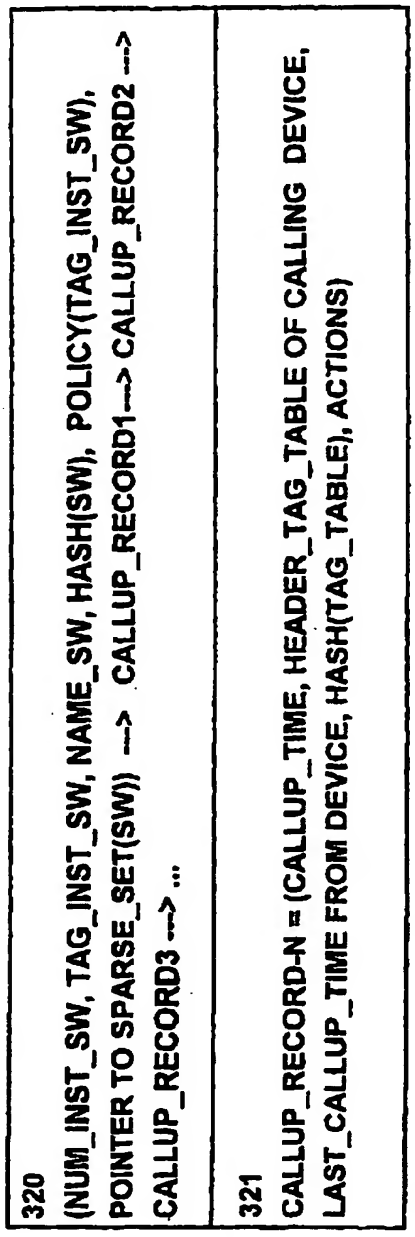

270
ソフトウェアの
インスタンスの
呼び出しをユー
ザーが要求する。
271
要求された
ソフトウェアの呼び
出しを管理プログラ
ムが遮る。
272
呼び出しが必要で
あるかを管理グラム
が決定する。
NO
YES
274
要求された
インスタンスのステータ
スの継続を決定する。
278
呼び出しポリシー内
の呼び出しであるか?
継続
GC_DISABLED
YES
NO
279
ユーザー装置への
報復措置実行
OPTIONAL
275
アクセス
許可
276
アクセス
拒否
273
呼び出し
処理を
実行する。
277
タグテーブル
を更新する。

使用管理手順

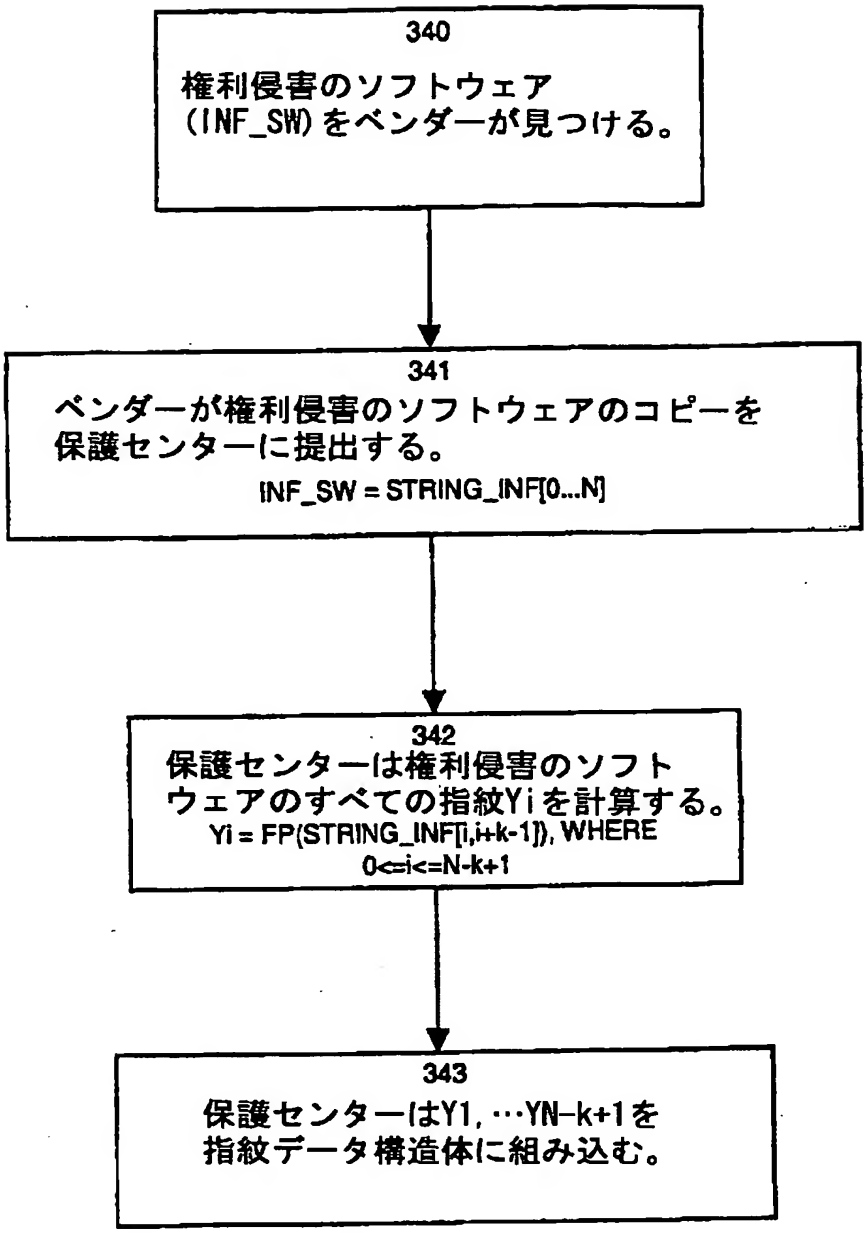
【図９】


通信ネットワーク100へ
103
保護センター
304
クロック
301
プロセッサ
303
相互接続機構
（モデム）
バス306
300
保護センターデータベース
137
指紋データ
構造体
138
タグのある
ソフトウェア
データベース
129
署名された
タグ
302
メモリ
315
検証プログラム
(VRP)
210
タグ
テーブル
126
指紋テーブル

【図１０】

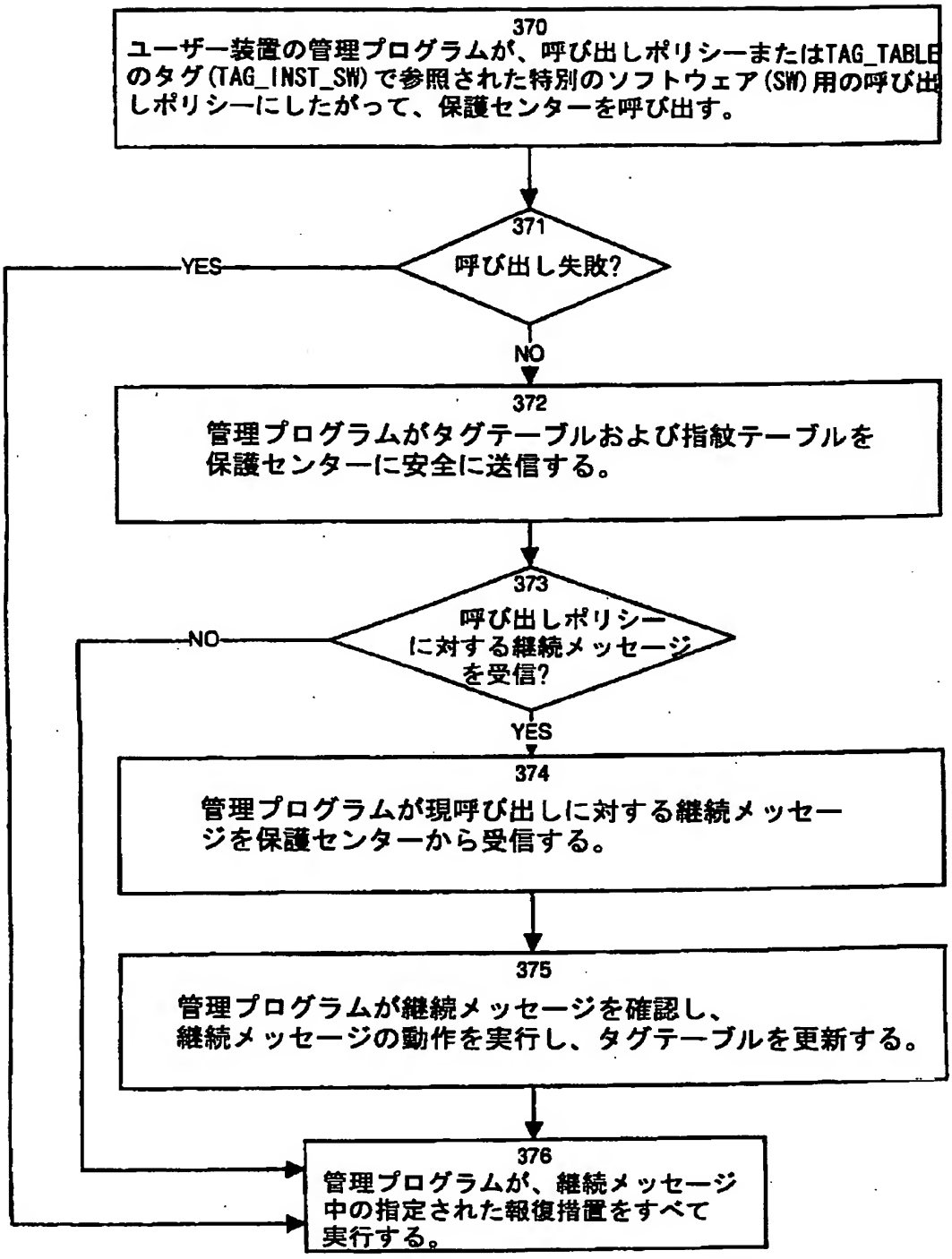

320
(NUM_INST_SW, TAG_INST_SW, NAME_SW, HASH(SW), POLICY(TAG_INST_SW),
POINTER TO SPARSE_SET(SW)) --> CALLUP_RECORD1--> CALLUP_RECORD2 -->
CALLUP_RECORD3 --> ...
321
CALLUP_RECORD-N = (CALLUP_TIME, HEADER_TAG_TABLE OF CALLING DEVICE,
LAST_CALLUP_TIME FROM DEVICE, HASH(TAG_TABLE), ACTIONS)
保護センターデータ

【図１１】



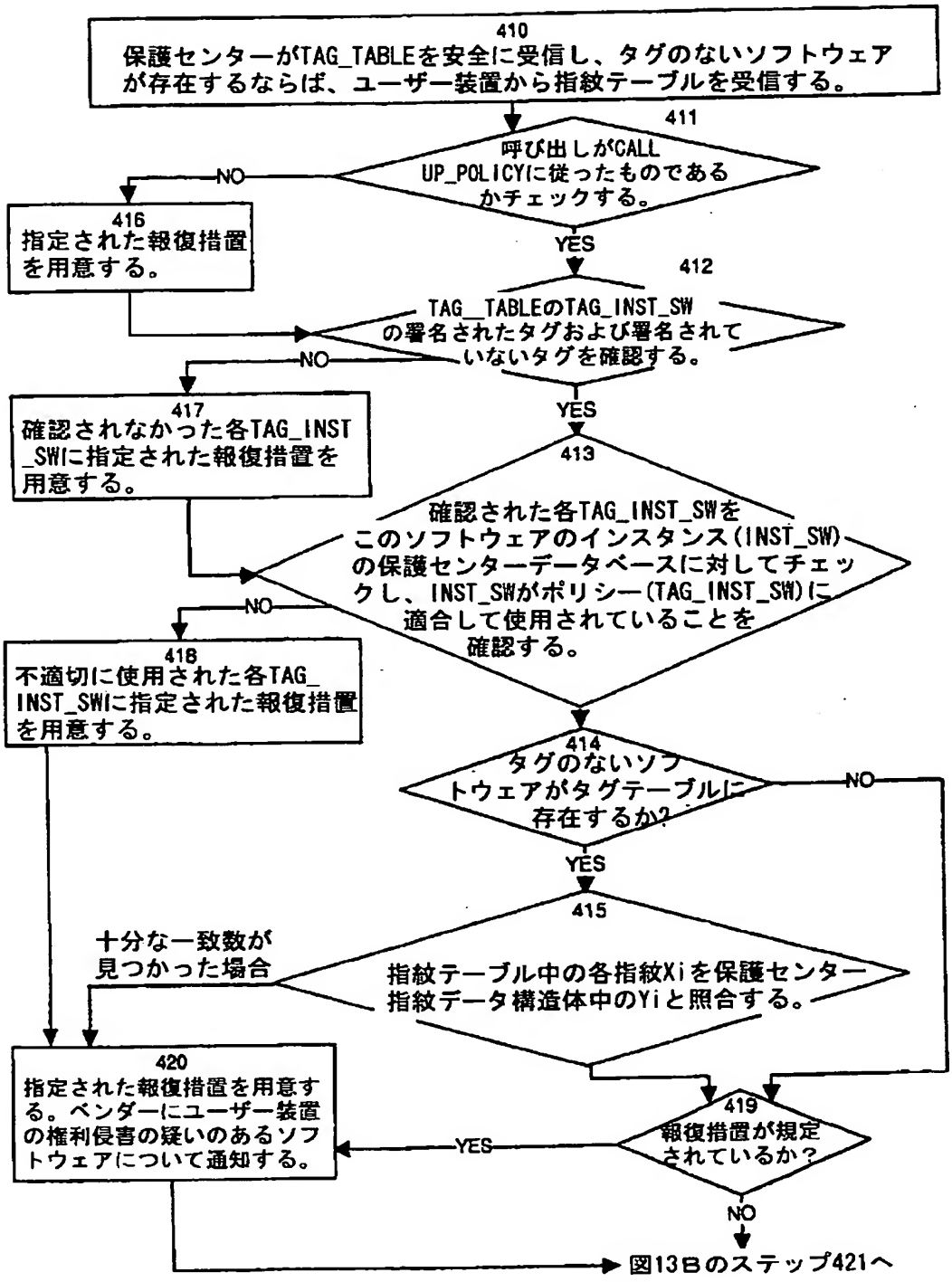
保護センターが権利侵害のソフトウェアを認識

【図１２】



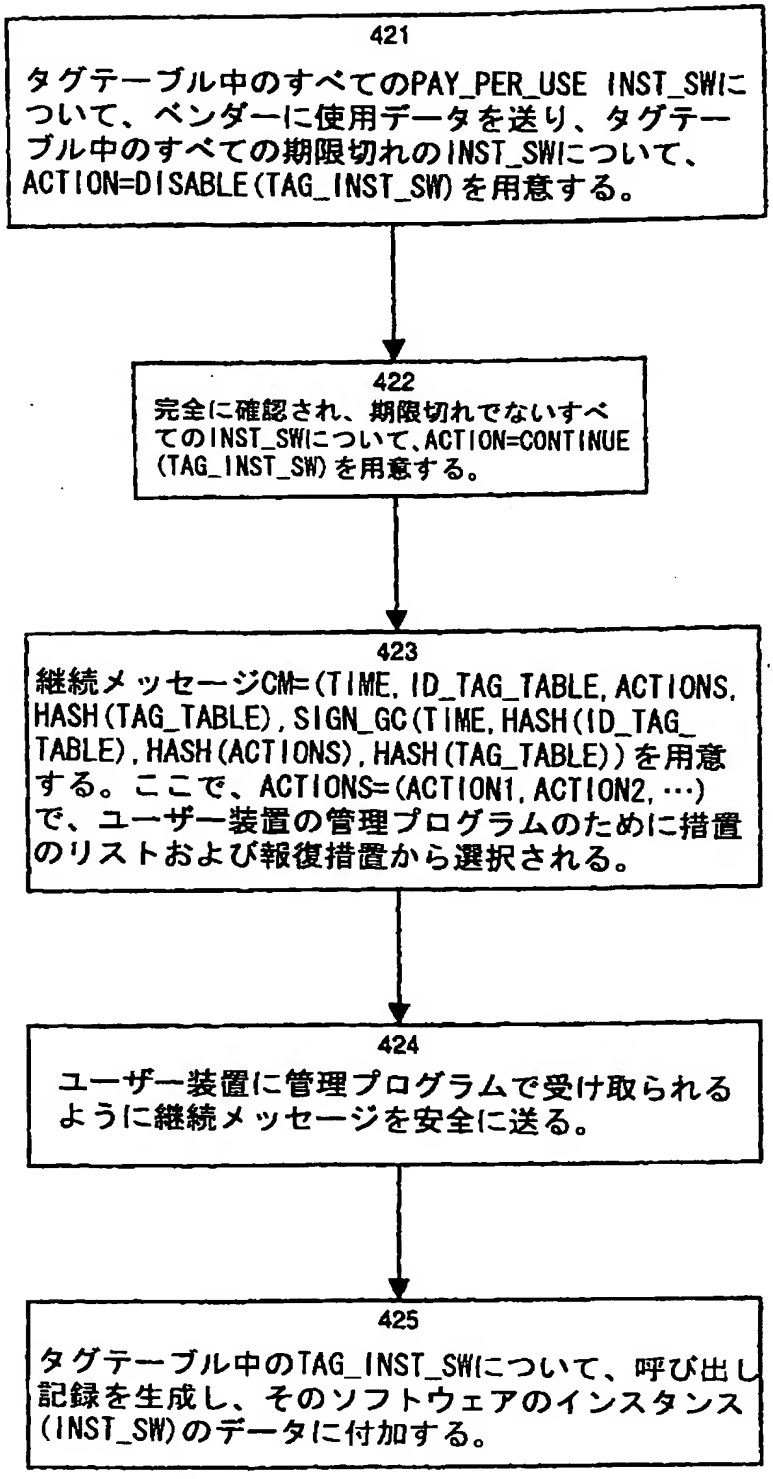
ユーザー装置から保護センターの呼び出し

【図１３Ａ】



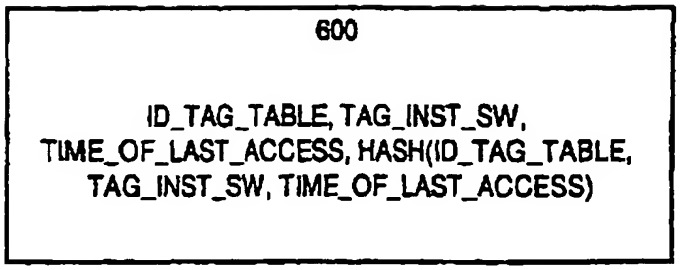
保護センター呼び出し処理

【図１３Ｂ】



保護センターに呼び出し処理

【図１４】



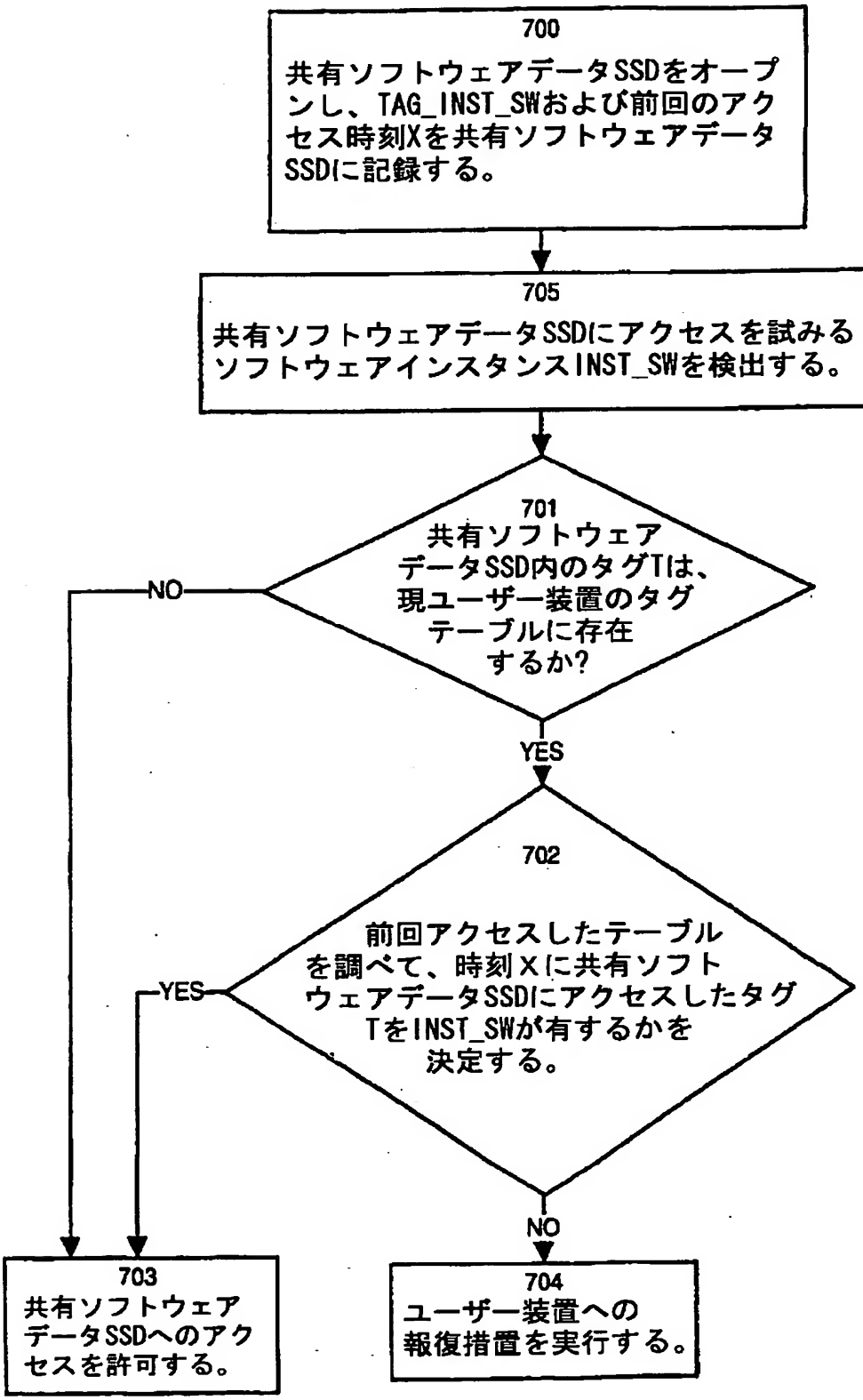
共有ソフトウェアデータと共に伝送されたデータ

601

タグ	アクセス時刻
TAG_INST_SW1	1999年 2月2日 午前 09:11 1999年12月2日 午前 07:24 1999年 2月1日 午後 09:36 1999年 2月2日 午前 11:17…
TAG_INST_SW2	1999年 1月 5日 午後 10:19 1999年 2月 8日 午前 08:34 1999年 2月 5日 午後 01:33…
TAG_INST_SW3	1999年 1月12日 午前 06:41

共有ソフトウェアデータSSDアクセステーブル

【図１５】


700
共有ソフトウェアデータSSDをオープンし、TAG_INST_SWおよび前回のアクセス時刻Xを共有ソフトウェアデータSSDに記録する。
705
共有ソフトウェアデータSSDにアクセスを試みるソフトウェアインスタンスINST_SWを検出する。
701
共有ソフトウェアデータSSD内のタグTは、現ユーザー装置のタグテーブルに存在するか?
NO
YES
702
前回アクセスしたテーブルを調べて、時刻Xに共有ソフトウェアデータSSDにアクセスしたタグTをINST_SWが有するかを決定する。
YES
NO
703
共有ソフトウェアデータSSDへのアクセスを許可する。
704
ユーザー装置への報復措置を実行する。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/US 00/11821

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 45768 A (NORTHERN TELECOM LTD) 15 October 1998 (1998-10-15) abstract; figures 1,3C,5 page 4, line 18 -page 5, line 32 page 6, line 38 - line 37 page 8, line 17 -page 10, line 24 page 11, line 7 -page 72, line 2 page 18, line 33 -page 19, line 18 page 20, line 26 -page 23, line 21 page 24, line 30 -page 25, line 26	57,58, 91,92, 111-114
Y		1-5, 7-12,59, 62-65, 93,96
	--- -/--	

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 October 2000	20.02.2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sigolo, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/US 00/11821

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 825 883 A (ARCHIBALD WILLIAM CHARLES ET AL) 20 October 1998 (1998-10-20) abstract; figures 2-4,6 column 4, line 1 -column 6, line 40 column 7, line 32 -column 9, line 67 column 10, line 57 -column 11, line 51 column 18, line 44 -column 19, line 39 column 20, line 41 - line 55	53-55, 57-59
Y		1-5, 7-12,59, 62-65, 93,96
A	US 5 823 907 A (JOHNSON HERRICK J ET AL) 11 June 1991 (1991-06-11) abstract; figure 1 column 2, line 49 -column 5, line 42	13-18

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int...ational application No.
PCT/US 00/11821

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-18, 53-70, 91-93, 96-102, 111-114

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

International Application No. PCT/US 00/11821

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-18, 53-70, 91-93, 96-102, 111-114

   System for monitoring usage of software, comprising a software vendor, a tag server and a user device running a supervising program

2. Claims: 19-35, 36-39, 74-90, 108-110, 115-118

   Centralizing control at a specific server of software usage at the client

3. Claims: 103-105, 119-131,134, 40-52, 71-73

   Intercepting use of unregistered instances of software

4. Claims: 106,107, 94,95

   Uniquely identifying instances of software prior distribution

5. Claims: 132-133, 135-137

   Limiting use of software on specific hardware devices

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. al Application No
PCT/US 00/11821

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9845768 A	15-10-1998	US 6108420 A	22-08-2000
		AU 6492198 A	30-10-1998
		CN 1255209 T	31-05-2000
		EP 0974084 A	26-01-2000
US 5825883 A	20-10-1998	NONE	
US 5023907 A	11-06-1991	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW

(72)発明者 ラビン・マイケル・オー
アメリカ合衆国, マサチューセッツ州 02138, ケンブリッジ, コンコード アベニュー 243

(72)発明者 シャーシャ・デニス・イー
アメリカ合衆国, ニューヨーク州 10012, ニューヨーク, ブリーカー ストリート 100

Fターム(参考) 5B076 FB03 FB05 FB19 FD01
5B085 AE26 BG07